2013-06

Examining the return on investment of a security information and event management solution in a notional Department of Defense network environment

Warnecke, Matthew P.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXAMINING THE RETURN ON INVESTMENT OF A SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION IN A NOTIONAL DEPARTMENT OF DEFENSE NETWORK ENVIRONMENT

by

Matthew P. Warnecke

June 2013

Thesis Advisor: Thomas Housel
Thesis Co-Advisor: Johnathan Mun

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
EXAMINING THE RETURN ON INVESTMENT OF A SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION IN A NOTIONAL DEPARTMENT OF DEFENSE NETWORK ENVIRONMENT

5. FUNDING NUMBERS

6. AUTHOR(S) Matthew P. Warnecke

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Sophisticated cyber threats represent a significant adversary in the evolving world of the cyber domain. Furthermore, determining whether or not an attack has taken place and the extent of the damage caused requires significant resources. In order to guarantee reliable detection, prevention and mitigation of these advanced threats, the Department of Defense (DoD) must invest in advanced information security technologies that increase the defensive capabilities of its information networks.

This thesis focuses on Security Information and Event Management (SIEM) systems as an enabling technology that possesses the advanced security capabilities required to address sophisticated, evolving cyber threats. The research explores the capabilities of this technology in terms of the speed of detection, depth of investigative power, and additional value provided. Additionally, this research attempts to quantify the return on investment that a SIEM solution could provide when deployed in a notional DoD network architecture. Ultimately, the research provided in this thesis endeavors to justify DoD investment in SIEM technology.

The focus of this research revolves around a qualitative description of the inherent capabilities of SIEM products and utilizes several Return on Security Investment models in an attempt to quantitatively define the value of these capabilities in a DoD network.

14. SUBJECT TERMS Security Information and Event Management, Security Event Correlation, Incident Response, Return on Investment, Return on Security Investment, Return on Security, Network Intrusion	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXAMINING THE RETURN ON INVESTMENT OF A SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION IN A NOTIONAL DEPARTMENT OF DEFENSE NETWORK ENVIRONMENT

Matthew P. Warnecke
Lieutenant, United States Navy
B.S., United States Naval Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2013

Author: Matthew P. Warnecke

Approved by: Dr. Thomas Housel
Thesis Advisor

Dr. Johnathan Mun
Thesis Co-Advisor

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Sophisticated cyber threats represent a significant adversary in the evolving world of the cyber domain. Furthermore, determining whether or not an attack has taken place and the extent of the damage caused requires significant resources. In order to guarantee reliable detection, prevention and mitigation of these advanced threats, the Department of Defense (DoD) must invest in advanced information security technologies that increase the defensive capabilities of its information networks.

This thesis focuses on Security Information and Event Management (SIEM) systems as an enabling technology that possesses the advanced security capabilities required to address sophisticated, evolving cyber threats. The research explores the capabilities of this technology in terms of the speed of detection, depth of investigative power, and additional value provided. Additionally, this research attempts to quantify the return on investment that a SIEM solution could provide when deployed in a notional DoD network architecture. Ultimately, the research provided in this thesis endeavors to justify DoD investment in SIEM technology.

The focus of this research revolves around a qualitative description of the inherent capabilities of SIEM products and utilizes several Return on Security Investment models in an attempt to quantitatively define the value of these capabilities in a DoD network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

SIEM	Security Information and Event Management
SIM	Security Information Management
SEM	Security Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DoD	Department of Defense
ALE	Annualized Loss Expectancy
CTM	Critical Threat Multiplier
EF	Exposure Factor
SLE	Single Loss Expectancy
ROI	Return on Investment
ROSI	Return on Security Investment
ROS	Return on Security

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my wife, Lauren, who has always supported me throughout every endeavor, academic or otherwise, and has always been my biggest source of inspiration.

To my son, Grant, for teaching me humility, patience and unconditional love.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Emerging cyber threats indicate a significant obstacle to Department of Defense (DoD) assets and operations worldwide. Contemporary information assurance strategy promotes a defense-in-depth paradigm, where network security devices exist in layers to counter specific threats or monitor specific activity. Further, financial justification for these investments hinges upon the notion of security as a cost of doing business. However, in an era of limited budgetary consideration for computer network defense investments, funding a new implementation of a security investment requires not only a dynamic range of prevention and incident response capabilities, but must also provide an acceptable return on investment (RoI).

In the DoD, this presents a unique situation that juggles capability enhancement versus the sunk cost of a security investment. After all, an investment in security represents a sunk cost because it does not generate revenue for the organization (Stephenson, 2012). But, justification of an investment in security resides in the avoidance of potential costs that the capability aims to mitigate or minimize.

A Security Information and Event Management (SIEM) implementation offers the ability to leverage the current defense-in-depth- strategy employed throughout the DoD while also offering increased defensive capabilities to further secure DoD networks and information systems. Furthermore, an investment in SIEM technology exhibits the potential for a significant return on security investment (RoSI) because of the enhanced capabilities offered inherently within the technology as well as the ability to correlate data from disparate network and network security devices, thereby increasing their effectiveness. Essentially, SIEM closes the gaps between the layers of a defense-in-depth security architecture and combines disparate security devices into a nimble, cohesive defense.

Despite the potential that SIEM technology represents to increase DoD network security, agility and efficiency, investment in the technology still requires quantifiable justification. However, as the typical measurement used to justify investments fails to apply to both the DoD as an organization as well as the security realm, exploring alternative measurements of calculating return require thoughtful consideration. Furthermore, an examination of several Return on Security (RoS) or Return on Security Investment (RoSI) methods offers insight into justification of an SIEM solution as well as a basis for considering future security investment options.

A. PROBLEM STATEMENT

Modern information systems face significant and sophisticated threats on a persistent basis. Traditional methods of thwarting cyber threats involve the application of perimeter security devices as well security solutions designed to mitigate specific threats. While altogether effective, this method leaves significant gaps in the ability to detect or prevent exploitation. Furthermore, most attacks go unnoticed for large amounts of time or until significant damage has already occurred. In order to effectively mitigate modern cyber security threats, organizations must consolidate security efforts into a single cohesive effort.

B. PURPOSE AND THESIS STATEMENT

The purpose of this study is to understand the value a SIEM solution can provide, both economically and operationally within a nominal DoD environment. Effectively, how can a SIEM application enhance network security and mitigate the risk of advanced cyber threats? Secondly, what potential return on investment could a SIEM application implemented on a DoD network provide?

On the surface, SIEM applications improve network security by integrating isolated network security devices via the aggregation and correlation of their associated log data, effectively forcing a potential attacker to attempt to bypass all security devices at once rather than individually. Despite this remarkable benefit, the value of a SIEM solution in a DoD environment must not only provide

increased capability, but also remain economically justifiable. This study will utilize various methods to determine the economic value of a SIEM solution, while also qualitatively determining the additional value provided by the system in the form of capability enhancement and increased knowledge of the host information system. Ultimately, this thesis will attempt to answer the questions a SIEM application enhance network security and mitigate the risk of advanced cyber security threats?

C. BACKGROUND

1. Threats Facing the Nation

Growing interconnectivity and information sharing capability brought about by networked information systems has changed the way that Americans communicate, conduct business and even view the world around them. However, increased reliance on information systems also represents one of the largest threats to the nation, primarily due to the evolution of advanced security threats. The sophistication and proliferation of cyber security threats throughout the world demand increased vigilance to innovate new methods to detect and mitigate them before they cause harm.

Federal agencies are not immune from these threats, but the detective and preventative capabilities across the nation are significantly lacking. For example, in 2012, 92% of security breaches were not detected by the affected organization and required a third party to determine that a breach had in fact taken place (Honan, 2012). Furthermore, most of those breaches were avoidable because the attacks themselves were not highly difficult to accomplish (Honan, 2012). However, the most staggering statistic of all from the data collected in 2012 is the fact that 85% of these breaches took at least one week to discover (Honan, 2012). Applying these statistics to the understanding that in 2011 federal agencies reported a total of 42,887 security incidents creates even more uncertainty surrounding the effectiveness of current network security measures (Wilshusen, 2012)

Federal systems are not sufficiently protected to consistently detect or mitigate advanced cyber security threats (Wilshusen, 2010). Effectively intrusion detection and prevention requires advanced capabilities not found within the current federal information security architecture. It is only through investment in enabling technologies like SIEM solutions that federal agencies have any hope of mitigating advanced cyber threats. This is of particular concern given the recent observation of malicious software affecting physical damage in the real world (Constantine, 2011). Malicious software and enterprising hackers can do more than just steal information, disrupt operating systems or evade perimeter security devices, and advanced security tools must increase their detective and preventative capabilities in kind.

2. DoD/National Cyberspace Strategy

The DoD maintains that cyber space is a critical war-fighting domain that requires continued attention to provide security to U.S. interest and maintain continuity of operations. The National Strategy to Secure Cyberspace explicitly defines advanced network security as a critical requirement, emphasizing the requirements to "prevent cyber attacks against America's critical infrastructure, reduce national vulnerability to cyber attacks and minimize damage and recovery time from cyber attacks that do occur" (Office of the President of the United States, 2003). In order to accomplish these requirements the nation must develop advanced cyber security intelligence that offers enhanced trend analysis related to evolving threats and vulnerabilities (Office of the President of the United States, 2003). Furthermore, as defined in the DoD IT Enterprise Strategy and Roadmap, these capabilities will enable the DoD to bolster its predictive and preventative capabilities, reducing the risk of successful attacks on data and networks (Officer of the Secretary of Defense, 2011).

Application of a SIEM solution also advances the special IT initiatives defined in the DoD IT Enterprise Strategy and Roadmap in several ways. Primarily, the SIEM application will drastically improve the cyber security situation

awareness across the department. However, as existing network security architecture focuses primarily on securing the perimeter of the DoD network, phased replacement of these systems would allow for a SIEM implementation in concert with a system refresh, advancing the capability to combat emerging threats and advance perimeter and enterprise wide security initiatives.

Additionally, the DoD endeavors to cultivate capabilities inherent in SIEM applications, as defined in the DoD Strategy for Operating in Cyberspace. SIEM solutions offer the DoD the ability to leverage automated tools and continual assessments against perimeter security efforts as well as internal monitoring and information management, which are in line with the DoD strategic initiatives (United States Department of Defense, 2011). Furthermore, employment of a SIEM represents a movement toward active cyber defense capabilities to discover, detect, analyze and mitigate threats in real-time (United States Department of Defense, 2011).

3. DoD Budget

Despite an austere fiscal horizon, securing defense information networks from intrusion is one of the critical areas highlighted for investment in the coming fiscal years (United States Department of Defense, 2013). As a national priority, continued investment in advanced network security requires not only innovation, but also strategic investment in capabilities that complement and support existing security investments. By leveraging the information provided by existing IT security investments throughout the DoD, a SIEM solution represents a security investment that not only enhances capability but also preserves and increases the value of the existing network security endeavors.

4. Benefits of the Study

The potential benefit of this thesis study includes economic justification of a security technology investment as well as an increased understanding of the inherent value provided by a SIEM solution. In addition to the financial incentive determined through this thesis study by determining the potential RoI of a SIEM

solution, this thesis will also describe operational benefits achieved through SIEM solutions such as increased network efficiency, enhanced compliance enforcement, threat detection and prevention, and an overall increase in real-time knowledge of the information system.

5. Security Information and Event Management

The forerunners of the technology that became Security Information and Event Management (SIEM) systems first arrived on the market in the early 1990s (Chuvakin, 2010). Effectively, SIEM solutions represent a combination of advanced log management systems and security event detection and notification. When combined, both of these technologies, known separately as Security Information Management (SIM) and Security Event Management, respectively, offer the ability to actively detect and investigate potential security threats in near real-time. In order to effectively accomplish this, the knowledge that each device creates about a network through extensive log files is combined into a single cohesive picture of the information system, allowing managers to distill threat patterns from disparate events from the aggregated, correlated data.

Originally, the premise of SIEM applications was explored in interest in order to reduce the number of false positives encountered by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (Chuvakin, 2010). However, as log file management systems achieved greater capability and efficiency, these applications developed into more of a security management solution, increasing the detective and preventative capability of any security architecture by combining their individual efforts into a single cohesive force.

Fundamentally, the application of a SIEM solution to a network provides absolutely no additional security (Dorigo, 2012, 2012). The stimulus for installing a SIEM solution comes from the added knowledge of the network and systems connected to it that the SIEM inherently provides. This knowledge can be used to effectively identify threats, provide compliance reporting, assist in forensic or

diagnostic investigation as well as offer a number of other advanced security operations.

6. Methodology

Initial research methods will primarily involve secondary research focused on SIEM technology and valuation of information security investments. These efforts will include case studies of SIEM solutions, descriptions of the capabilities provided by SIEM technology, and a comparative analysis of existing methods of determining the return on security investment.

Additional research to expand the subject as it relates to DoD network security will attempt to justify the investment in a SIEM solution by examining the results of an investment model applied to the implementation of a SIEM solution in a notional DoD network.

7. Thesis Structure

This thesis is organized into the following chapters.

Chapter I provides an introduction and overview of this thesis.

Chapter II gives a synopsis of SIEM solutions. This chapter provides a basic overview of the definition of SIEM, its background and components as defined by the current market state of the technology.

Chapter III describes methods of estimating return on a security investment. This chapter provides detailed descriptions on the various developing models of valuing investment in a particular security technology.

Chapter IV describes the application of a Return on Security Investment (ROSI) model to a SIEM solution in a DoD environment. This chapter describes the potential return on investment that a SIEM solution could provide when implemented in an environment similar to most DoD network environments, as well as the potential added benefits that the system provides.

Chapter V concludes this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SECURITY INFORMATION AND EVENT MANAGEMENT

A. BACKGROUND

1. Traditional Information Technology Security

Current methods of enterprise information technology (IT) security revolve around the application of point defense systems in a defense-in-depth strategy. While this strategy stands the test of time, as nation states have known for centuries that point security measures, such as border controls and passports, have a quantifiable effect on the overall security of the nation, it remains inherently flawed (Tarzey & Longbottom, 2012). Point defenses fundamentally mitigate a single vulnerability, or a single type of vulnerability. However, in a world of evolving advanced cyber threats, appliance security systems fail to address the overall risk of attack and leave systems vulnerable. Effectively, leaving disparate security devices in isolation removes the ability to leverage the information they produce, and reduces their overall effectiveness at combatting the risk they were intended to mitigate.

The most troubling aspect of the traditional IT security practices remains the fact that the application of point security products provides no collective mitigation of risk. Essentially, the whole is lesser than the sum of the parts. For example, an intrusion detection system (IDS) or intrusion prevention system (IPS) may prevent multiple failed attempts to access a resource, but may miss the single successful penetration from the same source (Tarzey & Longbottom, 2012thm). Or, a virus scanner may protect a system from multiple attacks by malicious code, but may not detect a zero-day exploit. The result of traditional IT security strategy is that every security incident that is detected is addressed in isolation from the perspective of the intended security product based on its "inherently limited knowledge of its relation to other security incidents" (Tripwire, 2012). The application of a defense-in-depth strategy through point security devices effectively creates a scenario where an intruder can attack an

information system by learning how to evade each individual protection, having learned how to penetrate the preceding device (Swift, 2006). The downfall of each security product lies in its isolation from other security products. An intruder need only have the patience to develop a method to bypass each individual device and the entire security strategy crumbles.

Historically, application of IT security boils down to a singular factor, cost. In effect, security is about “managing risk at some cost” (RSA, 2010). Often, the most cost effective method of managing IT security risks is with the application of point security products aimed at mitigating specific threats (Tarzey & Longbottom, 2012thm). The amount of cost incurred to apply these point security products relates directly to the inherent value of the assets at risk. Furthermore, the current approach to costing these products is based on the deliverables provided at each point device. Effectively, the cost of managing the risk of cyber threat equates to the “number of scanners or monitors in use” and the value provided by the “amount of time they spend scanning or monitoring” (Tripwire, 2012).

This trend of managing IT security risk through application of point devices stifles the strategic potential of enterprise IT security. Further, failing to recognize the strategic importance of enterprise security relegates the application of it to a “jumble of silos – among them [Information Assurance Management], application security, endpoint protection, network security and data security” (Tripwire, 2012). The popularity of point security systems also suppresses the shift toward enterprise IT security because of the simplicity of these devices. The effort involved in the installation and management of point security products is almost negligible (Chuvakin, 2004). For example, the installation of a lock in the front door of a home provides a measure of security against intruders and is simple to install and manage. However, this point security device thwarts the risk of an intrusion only enough to force an intruder to discover another method of entry into the home. In order to effectively minimize the risk of advanced cyber threats,

organizations must recognize that protection entails moving beyond traditional point security products (Tarzey & Longbottom, 2012).

A more comprehensive approach to enterprise IT security must assert itself over the more traditional, disjointed methods. Vulnerabilities can no longer be considered in isolation. One cannot count of the individual devices to confer with one another on the significance of a group of events from disparate systems, nor can one rely on the ability of a security analyst to recognize the significance of individual events across security platforms (Hutton, 2007). In order to effectively mitigate the existing risk of exploitation that each point security device is intended to thwart, all of these assets must be aggregated and correlated across the entire enterprise network (Stephenson, 2012). Effectively, the integration of each point security device into a comprehensive approach enables advanced security intelligence, “improved analytics and optimal decision-making” (Tripwire, 2012).

2. Advanced Threats

Modern cyber security threats represent sophisticated, committed forces that are proven effective against existing security point defenses. In fact, there are many existing threat that have recently emerged “that can only be detected by correlating information from a wide range of sources, including point security products themselves” (Tarzey & Longbottom, 2012). Furthermore, if an attack represents an aspect of a broader campaign than the application of countermeasures may exceed the realm of enterprise IT security. However, in order to effectively combat these campaigns, application of countermeasures beyond the scope of IT security still may require information collected and correlated by IT security products (Tarzey & Longbottom, 2012). Effectively, combatting advanced cyber security threats requires more consideration than simply a tactical application of point security devices. Combatting modern, advanced cyber threats requires an integrated approach to security that leverages strategy rather than tactical proficiency.

3. Alternate SIEM Adoption Trends

Implementation of SIEM systems represents a trend toward solving a number of enterprise IT problems. Traditional SIEM, combined with log management technology, has the potential to deliver a multitude of functionality to the enterprise, from security incident response to regulatory compliance, system management and application troubleshooting (Chuvakin, 2010). Overall, the application of SIEM delivers advanced knowledge about the IT landscape that can deliver results in a number of different ways.

Log management functionality inherent in SIEM applications is another driving force in the adoption of SIEM systems. Every device, application and interface generates log data. SIEM applications allow organizations to efficiently manage these logs, offering not only collection solutions but also the ability to conduct comprehensive review of these logs lending immense knowledge of the IT environment to network managers. Furthermore, effective log management in SIEM applications streamlines the entire process, allowing organizations to easily and routinely collect, store and review logs at any point, not just after an incident (Chuvakin, 2010).

In addition to security applications, one of the primary drivers of SIEM application adoption is the capability that the technology lends to meet external compliance goals. There are multiple legal requirements imposed upon organizations that require effective management of log files. In fact, meeting regulatory compliance requirements is the main reason for 80% of all SIEM projects (Karlzen, 2009). Nearly every organization operating an information system on a network must meet baseline requirements for log file management, according to several legislative articles. The Payment Card Industry Data Security Standard (PCI DSS) mandates specific logging details including log retention and daily log review (PCI DSS). The Health Information Portability and Accountability Act of 1996 (HIPAA) requires log management for securing electronic protected health information (HIPAA). Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires log management

in order to maintain successful and efficient log management infrastructures, to include generation, analysis, storage and monitoring (44 U.S.C. CHAPTER 35, 2002). A SIEM implementation underpins the effort to achieve any internal or external regulatory compliance goal.

From a security standpoint, organizations adopt SIEM technology in order to develop a comprehensive knowledge base of the entire IT security architecture. One of the biggest obstacles that organizations faced was that they could not objectively discern whether or not an attack had taken place without significant effort. Adding a SIEM security implementation helps to mitigate this by reducing “the number of security events on any given day to a manageable, actionable list and to automate analysis such that real attacks and intruders can be discerned” (Swift, 2006). Further confusing the issue, different devices might report the same event on the network in a different way, increasing both the number and complexity of security events and leaving no way to discern the truth of their relationship (Chuvakin, 2004). Automating the correlation of disparate security events significantly alleviates the strain on security engineers, whom, no matter how skilled, are generally only able to respond to about 1,000 events per day (Swift, 2006). Furthermore, security applications of SIEM systems also leverage the potential of disparate security devices where, if events are not monitored and correlated, the “total security capabilities of a system will not exceed its weakest link” (Swift, 2006). Application of an SIEM system aids in integrating traditional network management and effectively increases the capability of detecting and responding to network security threats.

Furthermore, SIEM adoption trends by organizations represent a shift in the fundamental understanding of enterprise IT security. A recent RSA study noted that more than 75 % of mid-size organizations ranked real-time security monitoring as essential to their operations, and 90 % of the total respondents implemented SIEM solutions citing security operations as the primary purpose (RSA, 2010). SIEM represents the next step in advanced network security through its aggregation and correlation functionality as well, lending capability to

organizations through intelligent security systems. Effectively, the move away from scanning and monitoring unrelated security silos toward a more integrated approach represents the growing push toward enterprise security intelligence (Tripwire, 2012).

The strength of SIEM as a security application resides in the aggregation and correlation engine of the system. Before SIEM, terabytes of log data were available but unused (Sc eBook, 2010). By processing and correlating the immense amount of data produced by network devices, SIEM applications display the suspicious activity that humans simply could not discover and effectively aids in mitigating cyber threats that otherwise would have gone unnoticed (Tarzey & Longbottom, 2012). It was the lack of advanced security intelligence that lead to the tactical method of deploying point security devices, which can help secure networks. But, the capability to aggregate and correlate data offers organizations the ability to recognize that a device is being used in an unusual way in the context of the broader network (Tarzey & Longbottom, 2012). This capability is the cornerstone of SIEM adoption trends, taking existing intelligence and correlating it with other sources of information in order to foster good decision-making. Integration and correlation expands the breadth of security detection and protection, delivering improved security and advanced business value (Tripwire, 2012).

B. DEFINITION

1. Log Management

Log file management systems provide access to a source of information that lies unused in many network management solutions. Every device, application or system connected to a network produces log files containing information on the network connection or logging interaction between devices (Chuvakin, 2004). Security devices are particularly guilty of added to the ocean of information accumulated in log files (Hutton, 2007). However, the log files by themselves are irrelevant. Any program can scan log files, from the simplest

script to high-end applications (Dorigo, 2012). Effective log management includes comprehensive log collection, aggregation, retention, analysis and presentation (Chuvakin, 2010). Essentially, these defining features of a log file management system enable it to collect gigabytes and even terabytes of log data efficiently and deliver provisions to store it effectively and conveniently. This is not a trivial task as effective log file management is the first step toward a full SIEM environment (Dorigo, 2012). Without the ability to store and access these huge amounts of data effectively provided by log file management systems, SIEM capabilities would not exist.

2. Security Information Management and Security Event Management

SIM and SEM systems are the precursors for modern SIEM applications. SIM systems represent the log file management aspect of the SIEM architecture while SEM systems evolved out of network anomaly detection and notification systems. SIM focuses on analysis and reporting of log data and efficient storage with provisions for long-term storage and maintaining accessibility (Dorigo, 2012). Similarly, proper deployment of SEM tools also leads to a dramatic increase in the ability to effectively identify an incident in progress through real-time monitoring and notifications. However, the combination of these two systems together leveraged the power of log file analysis with anomaly detection, providing definitive data on real-time security events through integration and correlation. Essentially, it is the “events that trigger alerts, but it’s the information that gets the analysis done” (Stephenson, 2012).

3. Security Information and Event Management

Security Information and Event Management (SIEM) represents the combination of several research fields, including statistics, data mining, data warehousing, distributed data, machine learning and intelligent systems (Dorigo, 2012). Effectively, the combination of Security Information Management (SIM) and Security Event Management (SEM) consolidated the benefits of log file

correlation through log management systems in addition to leveraging anomaly detection into a single application. The technology to do this has existed since the late 1990s and was pioneered in order to develop a “security single pane of glass” (Chuvakin, 2010).

SIEM tools evolved out of the IDS and IPS disciplines. Early SIEM tools were developed in order to collect data from security devices in order to search for patterns indicative of threats (Sc eBook, 2010). Primarily, their original use in the IDS/IPS environment was to reduce false positives, which plagued network IDS/IPS systems at the time (Chuvakin, 2010). However, through their ability to effectively administer the data provided by security devices, they evolved into more of a security management tool.

The primary functionality of SIEM systems is to provide real-time analysis of security events captured by network devices (Aguirre & Alonso, 2012). These devices can be hardware or software, but the emphasis remains on the swift collection and correlation of data across these products in order to facilitate real-time monitoring and incident management (Gartner, 2011). An effective SIEM system combines the functionality of a centralized log file management system and analysis of these logs in real-time into an integrated product.

Done well, an SIEM application produces undeniable benefits. However, the most unique factor of SIEM applications is that they are not inherently security applications. Applying a SIEM solution to a network will not make a network more secure (Dorigo, 2012). However, when implemented properly, like an IDS system, a SIEM system can prove extremely effective at alerting anomalies and identifying threats, and other advanced security operations (Honan, 2012). While operational efficiency and effectiveness and log management are the goals of a SIEM implementation, the primary benefit of a SIEM product is the knowledge of the IT landscape of an organization that it creates (Dorigo, 2012).

4. Fundamental Aspects of SIEM

At the core of the functionality of SIEM products lies the ability to take lots of data from lots of different sources and distill “useful, actionable information from it” (Stephenson, 2012). For that reason, no SIEM tool can exist in isolation. In order to achieve the full functionality desired of an SIEM it must be able to interact with as many devices as possible on the network. Fundamentally, the primary functions of SIEM include log consolidation, threat correlation, incident management and reporting (Swift, 2006). In fact, the ability to correlate data is the defining feature of a SIEM tool, but it cannot be accomplished without aggregation of large amounts of data from many sources and continuous monitoring of events (Aguirre & Alonso, 2012). Effectively, the central aspect of a SIEM implementation is the ability to combine existing network resources into a “cohesive synergistic defense” (Swift, 2006).

C. SYSTEM FUNCTIONALITY

1. Collection

In order to provide the SIEM engine with data, it first has to be collected from the various devices in the IT landscape. Without information from devices on the network, the SIEM is effectively useless. Information is necessary to interpret the events and create knowledge about the network environment. Different SIEM implementations have different methods of employing software or hardware in the IT landscape in order to gather the required information.

In order to collect the data across the enterprise network, most SIEM systems utilize one of two particular methods involving agents. An agent is a particularly piece of programming provided by the SIEM vendor that is capable of forwarding log entries from a host to an SIEM collector over a secure connection (Dorigo, 2012). In the first collection method, an agent is installed on various devices like routers or firewalls throughout the network. These agents capture events processed by the devices on which they are installed and forward them to an intermediate device called collectors for normalization and aggregation. The

other method involves agentless collection where the “device is capable of sending the log entries to a collector themselves, thus mitigating the need for an agent to be installed” (Dorigo, 2012). Agentless collection has its advantages over collection through an installed agent because the device can run smoothly without interruption and without changes to its system (Dorigo, 2012). In order for a device with an installed agent to transmit the collected data to a collector it must intermittently disrupt the operation of the device upon which it is installed, which can have negative effects on the availability of network resources. However, the disadvantages of agentless collection are the facts that devices the lack encryption or compression methods and that the log file must be saved on the host system prior to transfer, which leaves information open to manipulation before arriving to the collector and uses finite resources on the host (Dorigo, 2012). Specific methods of collection usually vary depending on the sensitivity of the environment utilizing the SIEM system.

Collectors are the first step that data takes from the agents on the network toward the centralized SIEM system. They serve as an intermediate between potentially hundreds or thousands of agents around the network and the core of the SIEM application (Dorigo, 2012). Depending on the implementation, they can correlate some data, but their main purpose is to normalize the collected data from the various agents in order to forward more structured, hierarchal log data toward the core SIEM application (Dorigo, 2012). In addition to log data, collectors also gather contextual data on the environment in which the data was collected. This information can include network traffic statistics or user identity information as well as vulnerability assessment results (Chuvakin, 2010). Effectively, collectors accomplish the enormously difficult task of gathering data from every agent on the network, turning it all into something that can be read by the core SIEM application, and forwarding it on to the correlation engine.

2. Normalization

One of the primary obstacles that SIEM systems face before data arrives at the core SIEM application is the fact that each device on the network keeps logs in different formats. A Cisco router keeps logs according to a different schema than a Linux server and a workstation running Windows. Correlating the data contained within the logs of these three devices can be accomplished without normalizing the log file to a common schema, but that process becomes impossible once the system attempts to correlate the log files of hundreds or thousands of devices throughout the enterprise.

Because these file formats are often so different, before the log files collected can be "intelligently categorized, it should be normalized to a common schema" (Chuvakin, 2004). This formatted log data, now in either a universal or proprietary format depending on the vendor, is then forwarded to the core SIEM application.

3. Correlation

The ability to correlate data across disparate network devices is the primary benefit of SIEM systems. Relating different events and contextual data to each other helps sift through immense amounts of diverse data and identify problems, threats or potential attacks. From a security perspective, event correlation refers to the process of threat identification by "looking at not only individual events, but also at their sets, bound by some common parameter" (Chuvakin, 2004). For example, an event detected on a firewall may not be suspicious by itself, but when it can be associated with an escalation of user privilege or an upload of unknown software it then merits further investigation (Honan, 2012). However, without the ability to correlate log data like this than the pattern of events disappears in the ether of hundreds of thousands of network events.

SIEM correlation uses two loosely categorized methods in order to sift through the large amounts of data provided to the application that highlights the

realistic anomalies occurring on the network while at the same time reducing false positives. The first method, rule-based correlation, follows a similar methodology to signature based virus detection (Chuvakin, 2004). The second method employs the knowledge derived from normal network activity accumulated over time and then applies statistical correlation methods to this baseline (Chuvakin, 2004). Furthermore, both of these methods apply to data collected between events and known vulnerabilities, between events and characteristics of the host network and between events from different hosts on the network (Dorigo, 2012). All of these methods applied from each of these perspectives enable the correlation engine of SIEM applications to distill actionable information from hundreds of thousands of seemingly random events.

Rule-based correlation follows a pattern defined by existing knowledge of an attack (Chuvakin, 2004). The correlation engine determines then determines the severity of the threat based explicitly on what is detected in precise terms. Essentially, a series of in-then statements exists within the SIEM application delineating an exact scenario that an attack must follow in order to be detected as a high-severity threat (Chuvakin, 2004). The strength of rule-based correlation lies in the ability to uncover hidden threats or exploitations that are impossible to uncover otherwise, like the typical slow play attack employed by hackers over long periods of time.

Statistical correlation utilizes numerical algorithms to detect deviations from normal event levels and other routine activities (Chuvakin, 2004). Detecting threats through statistical analysis first requires careful base lining of network activity and the establishment of event thresholds (Chuvakin, 2004). Careful institution of these thresholds can help mitigate false positives, but depending on the tolerance of these thresholds it can also assist in detecting low volume threats. Although easy and logical to implement, the implementation of statistical correlation algorithms requires time to trend normal network and host activities, in addition to acceptance of these events as normal activity (Chuvakin, 2004).

Both methods of correlation have inherent challenges both in implementation and in their ability to detect patterns effectively. However, the combination of both of these methods effectively mitigates the shortcomings of them both, leading to coherent correlation and quality threat identification (Chuvakin, 2004). Additionally, effective correlation of collected log data allows security managers to uncover unforeseen attacks and thwart them in progress, should the data be provided to the core SIEM application quickly enough (Tarzey & Longbottom, 2012thm). But, regardless of the collection speed, these correlation methods can be applied to incoming events or historical data as necessary to determine the existence of a threat (Chuvakin, 2004). When done effectively, correlation of log data offers the promise of dramatically reduced response times for routine attacks, automation of threats detected through rules and statistics, identification of suspicious and malicious activities on the network and increased awareness of the network (Chuvakin, 2004).

4. Notification

The most useful feature of SIEM application is its ability to notify managers of what it detects. Reporting on the events that SIEM application observes takes several forms, depending on the threat classification of the correlated events. The initial intent behind SIEM applications was to provide managers with a “single pane of glass” view of their network (Chuvakin, 2004). Accurate, timely reporting from SIEM applications allows manager to effectively view network activity in real or near real-time. Additionally, depending on the severity of the detected threat, the SIEM application can notify management and security response teams via e-mail, SMS messaging, or even enact automatic security controls to mitigate the threat. These measures not only add value to the network, but also significantly increase the knowledge of the organization regarding the tools and services available on their information systems.

D. USE CASES

1. Models of SIEM Applications

Implementation of SIEM application usually follows several main themes, depending on the desires of the organization upon installation of the system. Security implementations, often referred to as threat management, focus on "detecting and responding to attacks, malware infection, data theft and other security issues" (Chuvakin, 2004). This particular implementation focuses on SIEM systems detective and investigative ability in order to achieve heightened security awareness and responsiveness. Another use case of SIEM implementations involves the desire of the organization to achieve regulatory compliance more effectively. This focuses on satisfying local policies as well as satisfying various laws and mandates (Chuvakin, 2004). Finally, organizations implement SIEM systems in order to advance their understanding of their information systems and networks. From this operations standpoint, organizations gain actionable knowledge of their networks in real-time (Chuvakin, 2004). Variations of these implementation themes exist, and organizations often install a SIEM application with the intent to achieve one, but eventually, often unintentionally, exhibit characteristics of all three examples.

2. Threat Management

Security implementations of SIEM systems allow for effective threat management across the enterprise. Collection and correlation of log files via a SIEM application reveals the vital signs of a network, providing a solid base for incident management and threat response (Dorigo, 2012). The realization that "the number of attacks against a network is never zero, nor is the number of suspicious transactions over the network," when compared against these observed vital signs allows SIEM applications to draw attack vectors and boost incident management capabilities of the organization (Dorigo, 2012). This is insight that cannot be derived from point security tools alone, and SIEM

applications can report on all of them effectively and in a timely manner in addition to reducing the impact of security incidents.

Another motivator of SIEM security applications is the ability to shield organizations from some of the most elusive and complex modern threats. For example, SIEM has the ability to counter insider threats because of the increased monitoring capability and improved identity and access management that the system provides (Karlzen, 2009). Effectively, every user from super administrator to guest access can be monitored swiftly and accurately with automated security controls preventing any unauthorized access or data leakage. Furthermore, SIEM systems have the innate ability to identify weak spots in a network security architecture, allowing security engineers to shore up defenses before they are exploited in real-time.

3. Compliance

SIEM implementations, thanks to their superb log reporting and management capabilities have become synonymous with compliance management systems (RSA, 2010). Effectively, SIEM systems can be configured to automatically enforce current policies and regulations as well as provide extensive log management solutions. Deviation from policy by any user or any device can be detected, correlated and corrected almost instantaneously and, more importantly, cost effectively.

For example, the National Institute of Standards and Technology published special publication 800–53, specifying the security and privacy controls for federal information systems and organizations (NIST, 2013). A SIEM application offers the ability to automatically determine compliance with these standards and generate the required documentation necessary to report this compliance.

4. Operational

The operational advantage and insight that SIEM implementations offer to organizations cannot be understated. SIEM systems provide automation of routine services, reducing the need for staff to conduct time-consuming and expensive data analysis (Tarzey & Longbottom, 2012). Additionally, SIEM applications boost confidence in IT systems, which allows organizations to effectively leverage the business value that IT systems provide. The confidence increase comes from the increased system protection that improves system availability, a more capable IT staff that is no longer burdened under the weight of thousands of potentially threatening events, and readily available information on network health and operations (Tarzey & Longbottom, 2012). However, the ultimate value that a well-deployed SIEM application provides is the improved business continuity and minimal operation and financial impact on services (Butler, 2009). SIEM applications provide the transparency required for seamless network operations in support of the organization while at the same time offer increased capability in protecting and monitoring these assets as well.

E. CONSIDERATIONS

1. Implementation

One of the pitfalls of implementing SIEM systems is the consideration that an SIEM system may not be the most practical solution to the problems found within an enterprise network. For example, in order for a SIEM application to function effectively, an organization must have established risk management objective, security policies and compliance requirements in order to achieve the most return on the investment (RSA, 2010). Otherwise the system will gather and correlate log data with no intended purpose, other than security management, and then the full value of the system never becomes realized. Another problem arises from the network configuration of the organization's network (Sc eBook, 2010). Just like other network devices, SIEM applications require tuning and adjustment in order to reach their full potential and provide the most value for the

organization. Common indications that the SIEM application is not performing effectively often include reports not accurately reflecting rule sets, or if other sources (mainly network administrators) are reporting incidents before the system has the opportunity (Dorgio, 2012).

Finally, the most important consideration during the implementation of a SIEM application is the status of log files throughout the network. Without log data, a SIEM application is essentially useless. Lack of log data often results from several common configuration errors, including not logging files at all, deleting log files too soon, incorrectly prioritizing logs, or even ignoring the logs, which commonly occurs with internal network devices when organizations only focus on the perimeter (Chuvakin, 2004). Often the most effective mitigation to this problem is to implement a log management system independent of a SIEM application prior to purchasing a SIEM solution in order to ensure that proper log management occurs before adding the ability to correlate log data.

2. Network and Hardware Issues

Implementation of a SIEM application can have particular effects on a network. Mitigating these effects requires that particular attention be paid to both the host network and the SIEM application capabilities. For example, incompatible hardware or insufficient software can limit the amount of data that a SIEM application receives and therefore limits the capability that it can provide. Furthermore, optimum SIEM performance requires that it consolidate as much data from as many sources as possible, which can prove difficult in even the most efficiently designed network.

Hardware issues are common occurrences during SIEM implementations. For example, log collection is generally measured is events per second (EPS) where a single entry in a log file correlates to one event. A generic enterprise network collects approximately 20,000 EPS over eight hours of an ongoing incident, which equates to approximately 576,000,000 data records (Butler, 2009). Conservatively estimating a 300 byte average size of each record

amounts to 172.8 gigabytes of data (Butler, 2009). Memory availability, with respect to storage and RAM capacities are a huge concern when contemplating SIEM applications. Furthermore, limitations in the hardware capabilities of devices can also limit the effectiveness of a SIEM application. As an example, an average high- capacity firewall can process approximately 100,000 EPS, which would indicate that the agent or collector responsible for this device would need to be capable of processing the same amount (Butler, 2009). However, in the event that the installed agent or collector in the SIEM architecture cannot handle these processing speeds, how does one determine which of these 100,000 events are significant? Hardware issues, and in particular memory issues, must be overcome in order to effectively implement any substantial SIEM solution.

Additionally, an organization must also consider its network capacity when installing a SIEM solution as well. Hundreds of gigabytes of data moving across a network in order to support a single application per day can choke the capability of any network, no matter how robust. Speed and capacity are the benchmarks of modern information networks, and anything that could potentially slow them down significantly detracts from their value (Butler, 2009). For example, installing a firewall is a prudent step toward achieving a more secure network, but when that same firewall limits the speed of the network from 10 Mbps to 3 Mbps, security comes at an unreasonable cost. Furthermore, while one can argue that no realistic scenario exists where every device on a network operating at maximum capacity and therefore sending the maximum EPS to the SIEM system, a large portion of these events can still create bottlenecks on the network. In order to maintain an effective SIEM solution that increases capabilities, the network must be able to support the additional load of SIEM data as well.

3. Ethical Considerations

The last remaining consideration in an SIEM solution involves the collection of large amounts of data. Raw log data collected by SIEM solutions

has the potential to contain a large amount of sensitive data. As such, privacy and compliance laws may limit the collection of this data or make it significantly more difficult to collect (Dorigo, 2012). Additionally, SIEM solutions do not just collect data from a selected group of sources, unless they are specifically configured that way. Collecting data from every device about every user has significant implications and can reveal a lot about what is going on within a network and who is doing what, which could potentially be considered an invasion of privacy (Dorigo, 2012). Furthermore, in order to mitigate the risk of privacy issues, additional considerations must be taken when storing log data from certain sources for long periods of time. These ethical issues must be considered when implementing a SIEM solution, and must be accounted for with additional resources and processing if necessary in order to ensure proper operation and compliance of the system and all of its products.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DETERMINING THE VALUE OF A SIEM SOLUTION

A. BACKGROUND

Investments in information security capabilities present significant challenges to organizations. Modern cyber threats have the potential to cause massive damage to information systems while at the same time burdening organizations with monetary damage, corporate liability and tarnished credibility (Cavusoglu, 2003). Additionally, effective metrics for determining the value of security investments as well as their potential return on investment are difficult to determine. Defining security investment metrics also proves difficult due to the dynamic nature of the security environment. Evolving threats and countermeasures generate massive amounts of confusion in security investment strategy, often leading organizations to follow a security investment strategy geared toward alleviating fear, uncertainty and doubt (FUD). This is of particular concern when the cost of cyber crime worldwide is measured in trillions of dollars, and the average security budget claims only a fraction of the IT investment budget.

Security investments, unlike traditional investments, are by definition incapable of generating revenue. Specifically, “no one buys a SIEM solution to generate revenue” (RSA – ROI). However, determining the best methods to mitigate the threats facing an organization is a difficult task with minimal budgets and a wide variety of security technologies in the market. Furthermore, added investment in security only provides so much capability before additional security measures become either ineffective or cost prohibitive (Cavusoglu, 2003). Effectively, determining the most prudent range of security capabilities is a multifaceted task, composed of risk assessment, technology architecture, policies and procedures (Cavusoglu, 2004).

Regardless of the method of justifying a particular security investment, the costs associated with a security breach continue to rise and, more importantly,

are becoming more frequent occurrences amongst organizations of all kinds. In a recent study of the cost of cyber crime in 2012, researchers discovered that the average annualized cost of cyber crime is "$8.9 million per year, with a range of $1.4 million to $46 million" (Ponemon, 2012). This cost also represents a 6% increase from the study conducted in the previous year. Furthermore, one hundred and four successful attacks were reported among the participating organizations per week, marking an average 1.8 successful attacks per company per week (Ponemon, 2012).

The cost of cyber crime also has lasting external costs associated with a successful breach of security systems. For example, a recent study uncovered that the announcement of a successful security breach also precipitates significant negative stock market reaction (Yayla & Hu, 2011). On average, a security breach results in a loss of 2.1% of the organization's market value within two days of the event (Cavusoglu, 2003). Furthermore, this activity often leads to a perception of low security at the affected organization, which can often lead to future or successive attacks, or may "signal to the market a lack of concern for customer privacy and/or poor security practices" (Cavusoglu, 2003). Effectively, in order to contain both the internal and external costs associated with a security breach, an organization must not only invest in an effective security architecture, but must also cultivate the perception of a robust security architecture. Ironically, the most effective way to ensure both of these requirements is through thoughtful and persistent investment in advanced security systems.

B. THE ECONOMIC VALUE OF INFORMATION SECURITY

1. Background

As the complexity of information systems increase in turn with the sophistication of the threats facing them, organizations continue to justify further investment in information security as merely a sunk cost. Most often, the value of a security investment, or even an existing security architecture can be difficult to quantify, thereby leading organizations to attempt to justify their expense through

qualitative means. These justifications lead to investment in information security on the understanding that security is a cost of doing business, or akin to insurance costs, or that security is one aspect of risk management (Lockstep, 2004). Despite these justifications, information security should be viewed as a "value creator that supports and enables" the organization, rather than simply just a cost of doing business (Cavusoglu, 2003). More effective methods of determining information security investment strategy often acknowledge the qualitative reasoning involved with security spending, but also utilize economic returns and technical performance to further enhance their decision making (Iheagwara, 2004).

Economic evaluation of a security investment remains the largest obstacle to implementing a new security technology. Measuring the return the investment could potentially provide is difficult because the methods of quantifying this value are determined by measuring the costs associated with something not happening to an organization. For example, the value of a firewall could be determined by the average costs associated with a security breach that were mitigated from the installation of the firewall. However, the value of the firewall remains unclear. The model for determining the RoI of the firewall cannot distinguish a mitigated attack from an attack that never occurred, so the value derived from not experiencing an attack is inherently ambiguous.

Further inquiry into the value of a security investment according to the existing methods of valuation also fails to acknowledge the security architecture as a whole. Economic evaluation of IT security investments often does not account for how different security technologies interact with each other, which is a significant issue in determining the value of a particular investment. Security controls throughout the IT architecture may substitute or complement others, but the true value of a security mechanism, with respect to the capability it provides, depends on the capabilities of the surrounding mechanisms (Cavusoglu, 2003). This is the basic tenant of a Defense-In-Depth strategy. Effectively, complementary technologies implies that the value of a security investment is

greater based on the deployment of supporting technology than if the technology was deployed alone (Cavusoglu, 2003).

Additional obstacles in determining the economic value of an information security investment deal primarily with the methods used to value the assets that a security device is intended to protect. Organizations place value on the assets in their inventory differently, whether they associate value of a breached computer as simply the replacement cost of the equipment, or whether they value the data contained on that device as well (Sonnenreich, 2006). Furthermore, the cost of a security incident is ambiguous as well. Costs associated with a security incident take many forms including cost of damage, the cost of responses to an incident, and operational costs (Iheagwara, 2004). This lack of standardization in valuation of assets and costs associated with security incidents often leads to inflated or abstruse results when determining the value of a security investment.

There are several strategies in use that attempt to provide a valuation of potential security investments. Among these are the time-tested strategies of Fear, Uncertainty and Doubt (FUD), extensive risk mitigation strategies, as well as attempts to determine the most affordable security available given a specific organization's financial constraints. Each of these strategies carries its own flaws and inconsistencies, primarily because they attempt to determine value in an investment that protects against loss rather than enables a measurable financial gain. However, in a world where information security threats are responsible for approximately $1.6 trillion in losses in the world economy and $266 billion in the United States alone, the need for a more effective method of determining the value of security investments continues to grow exponentially.

2. Fear, Uncertainty and Doubt

The Fear, uncertainty and Doubt (FUD) security investment strategy deserves acknowledgement because of the widespread utilization it enjoys throughout the information security industry. Often, the investment decision

regarding a specific security technology treats the solution like a black box expected to neutralize a newly discovered threat or mitigate some potential vulnerability. While this strategy does tend to provide some results, for example the application of virus scanning software has the ability to detect viruses when no scanner was used before, the continued use of this strategy cannot provide reasoned justification for future security investment. Effectively, this technique fails to provide managers with any insights into how the different variables associated with an IT security investment affect the "risk, expected loss, and likelihood," of a particular security solutions and the threats it attempts to mitigate (Cavusoglu, 2003). While it costs far less to initially implement security measures than to recover from a security incident, this strategy offers no insight on what security measures to invest in or what capability to encourage.

3. Cost of Deploying Security

Another historical information security strategy deals primarily with the costs associated with deploying a particular security solution or set of solutions. Mostly, an organization considers the budgetary allowance they internally provide for security investments, if any, and decides upon the most capability available at the pre-determined price. Effectively, this strategy boils down to asking the question "What is the most I can get for $X, given that I am going to spend $X?" (Cavusoglu, 2004). The primary limitation of this model exists in the amount determined by the value $X. It offers no insight to the organization of how much they should be investing in IT security, nor does it attempt to justify the approved amount of the IT security budget. Additionally, determining an IT security investment strategy simply by assigning available capital to the security budget does not provide any insight on the risk exposure that the organization faces or account for mitigation efforts that should be employed given the potential threats targeting the organization specifically. For example, an organization in the defense industry and an organization in the entertainment industry have wildly different threats targeting their information systems in addition to dramatically different vulnerabilities within their information systems. An IT security investment

strategy for both of these organizations should be tailored to specific needs of the organization, rather than simply what funding is available.

4. Risk Management

The most advanced method of crafting an economically justifiable IT security investment strategy relies on determining the likelihood of a specific security event taking place and the costs associated with this specific event. Profiling the existing risks that an organization is exposed to not only provides a more accurate understanding of the security capabilities the organization requires, but can also help determine the "optimal amount to invest in security controls" by "considering the vulnerability to a breach and the potential loss associated with a breach" (Cavusoglu, 2003). This optimal amount comes from estimating the expected loss from a security incident and determining that the level of investment in a solution to mitigate this vulnerability should cost no more than this expected level of loss (Iheagwara, 2004). Additionally, the value of this security investment strategy replaces financial metrics with mitigated risk as the primary deliverable, thereby adding value to the enterprise (Purser, 2004).

There are limitations to implementing a security investment strategy based on risk management. Primarily, these limitations arise out of the uncertainty inherent in the estimation of the costs of security incidents and their likelihood. Because of the rapid pace of technological development in IT, information security factors continue to change making it much more difficult to acquire an adequate amount of historical data to determine the true costs associated with exposure to a particular risk as well as its rate of occurrence (Chai, Kim & Rao, 2010). Also, the risk analysis associated with this particular strategy can show how a particular investment may not be economically justifiable, based on the amount of risk associated with a particular event. For example, investing enough to mitigate risk from very high levels or very low levels of vulnerability may not be economically justifiable or feasible (Cavusoglu, 2003). However, the fundamental flaw in a risk management based investment strategy is the fact that the

endeavor attempts to estimate how much an organization stands to lose from not investing in a particular security technology rather than how much it can benefit (Cavusoglu, 2003).

C. METHODS OF QUANTIFYING THE ROI OF A SIEM SOLUTION

1. Background

Quantifying a return on investment for information security solutions is inherently difficult because of the benefit that the security technology provides. Essentially, the purpose of a particular security solution is to prevent something from happening, and therefore avoid losses associated with that event. However, it is particularly difficult to measure these avoided losses because of the fact that they simply did not occur (Rosenquist, 2007). Furthermore, measuring ROI of network security devices proves even more difficult when attempting to accurately calculate the risk associated with a particular event because of the intrinsic subjectivity of network security events (Iheagwara, 2004). Major security events are rare occurrences, typically three or even six sigma events, but because of the subjectivity of these events, it is incredibly difficult to determine if a major security event was mitigated because of the inclusion of a new network security device, or if it never actually occurred.

The only factors of ROI that can be measured with a modest amount of certainty are the costs associated with a security investment. A SIEM solution, like all other information system investments comes with an assortment of costs including an acquisition cost, implementation costs, administration costs and maintenance costs (RSA –ROI). However, these costs do not account for the infrastructure costs or the agility costs, which deal with the degradation of prior investments and the inhibition of business, respectively (IANS, 2011). Therefore, even the costs associated with a security investment retain an amount of uncertainty, making it even more difficult to quantify the ROI of an investment.

The difficulty in measuring the ROI of security investments often leads to firms adopting subpar investment strategies, or investing in needless security

solutions. The difficulty in determining the ROI of security investments rests primarily on the difficulty in measuring the benefit produced by the security solution. Potential losses avoided are difficult to measure based on the probability of occurrence and also because “constantly evolving security programs, threats, and environmental changes limit the absolute accuracy of any predictive method based on historical trending data” (Rosenquist, 2007). However, despite the qualitative justification of many security expenditures, often the only way to justify a security investment to decision-makers is to show how investments impact the bottom line.

2. Cost Avoidance

The primary motivation to invest in any security solution is cost avoidance. Effectively, the decision to invest in a security solution is primarily driven by the fear of incurring losses associated with a security incident. However, the likelihood of a catastrophic cost avoidance scenario is incredibly low, which removes a great deal of the value attributed to the security solution (RSA – ROI). Furthermore, any analysis of a cost avoidance scenario based on single-point estimates is inherently flawed (Mun, 2010). Ultimately, the effectiveness of a cost avoidance model stems from its ability to engage non-technical stakeholders by attempting to quantify the qualitative benefits associated with good information security into a rudimentary financial benefits model (Lockstep, 2004).

The cost avoidance model can be further examined based upon the type of losses a security measure attempts to mitigate. For example, a security countermeasure can have one of two effects on a threat: “it can reduce the likelihood of the threat manifesting as an incident, and/or it can reduce the severity of the incident should it actually occur” (Lockstep, 2004). Effectively, avoided losses can be ascribed to either preventative security countermeasures or curative security countermeasures, deriving further incentive to invest in the solution.

3. Annualized Loss Expectancy

Another common method of determining the ROI of a security investment is to determine the Annualized Loss Expectancy (ALE). The ALE attempts to quantify the costs associated with a single security incident without countermeasures in place and with countermeasures in place. Effectively, this approach compares the untreated losses that an organization expects to face and compares those losses to the cost of the security investment required to mitigate these losses (Lockstep, 2004).

Calculating the ROI of a security investment utilizing the ALE model requires the calculation of a number of variables. First, the model calculates a Single Loss Expectancy (SLE) by determining the Asset Value (AV) and then multiplying it by the Exposure Factor (EF) and the Cascading Threat Multiplier (CTM) as shows in the below equation (Iheagwara, 2004).

$$SLE = EF \times AV \times CTM$$

The Cascading Threat Multiplier is used to more accurately determine the ROI of a security investment by estimating the impact that the threat has on other networked assets, known as the Underlying Exposed Assets (UEA) multiplied by a Secondary Exposure Factor (EFs) (Iheagwara, 2004). CTM is calculated using the following formula:

$$CTM = 1 + ((UEA \times EFs) \div AV)$$

Underlying exposed assets is measured in dollars and represents the assets that are now exposed due to the compromise of a specific asset (Iheagwara, 2004). Likewise, Exposure Factor (EFs) represents the secondary exposure factor related to the potential percentage loss of the underlining assets (Iheagwara, 2004).

The ALE is then calculated by multiplying the Annual Rate of Occurrence (ARO), predetermined by either observation or historical data, and by the SLE:

$$ALE = ARO \times SLE$$

ROI is determined by finding the difference between the recovery cost and the ALE, shown in the equation below. Where recovery cost (R) refers to the losses associated with in an environment where a security solution has not been deployed.

$$ROI = R - ALE$$

The ALE model provides many benefits to determining the ROI of a security investment, but the most compelling of them is its simplicity. Effectively, the model derives the potential value of a security investment through four simple equations and a few generalizations drawn from historical data or experience. However, moving away from its compulsion to adhere to single-point estimates and averages could enhance the model. Adding some variability into the model could assist in the justification of the investment by reducing some of the uncertainty in the actual cost of security incidents as well as their likelihood.

4. Return on Security Investment

Utilizing the Return on Security Investment (ROSI) model developed by Rosenquist follows several specific steps in order to accurately determine the value of a security investment. Determining the ROSI follows the following steps (Rosenquist, 2007):

- Evaluate cyber-attack incident data averages over time.
- Measure the reduction of incidents from implementing new security programs.
- Valuate the impact of avoided incidents.
- Apply the results to similar areas to estimate future value.

While Rosenquist's methodology has intrinsic value within it, the model does not allow for decision-makers to estimate the value of the security investment prior to implementation. The model does allow for comparative analysis between similar security investments, but the true value of the investment, following these specific steps, cannot be determined until the organization has the ability to observe a reduction in security incidents. Even then, the reduction in security incidents may not be directly attributable to the

new security device, thereby artificially inflating the value of the investment as well.

5. Return on Security

The Institute for Applied Network Security (IANS) developed an additional model attempting to quantify the value of a security investment in financial terms. Effectively, the IANS Return on Security (ROS) method "aims to correct the shortcomings of other cost-benefit analyses and produce a metric that is especially well suited to the unique qualities of a security project" (IANS, 2011). The IANS ROS attempts to provide this metric by expanding the area that the value of a security investment affects and specifically defining the costs associated with the investment.

The sources of value are defined as Objective Value (OV), Risk Value (RV), Infrastructure Value (IV) and Agility Value (AV) (IANS, 2011). Objective value refers to the achievement of a specific business goal. Risk value is defined as the reduction of risk. Infrastructure Value refers to the improvement of prior investments following the implementation of the security investment. Agility Value refers to the enabling of new business or business processes as a result of the improved security capability. The costs associated with the ROS model are defined as Objective Cost (OC), Infrastructure Cost (IC) and Agility Cost (AC) (IANS, 2011). Objective cost defines the price of purchasing, implementing and maintaining the security solution. Infrastructure costs attempts to define any degradation of prior investments as a result of the security investment. Lastly, Agility cost relates the impact of the security investment on the convenience of business processes or the development of new ones.

ROS is then calculated through the following equation:

$$ROS = (OV + RV + IV + AV) – (OC + IC + AC)$$

The primary issue with the IANS ROS model remains the uncertainty associated with estimating the values of each individual variable. Furthermore,

the values of AV and AC specifically may not be accurately estimated or measured until after deploying the security solution and observing the effects.

6. ROSI and ALE Hybrid Models

The Lockstep ROSI model effectively combines the output of the ALE model as well as the Australian-standard Threat and Risk Assessment (TRA) model in order to provide a common model that can account for statistical deviations (Lockstep, 2004). According to Lockstep, the model carries the following advantages:

- Financially quantitative
- Separates the contributions made to overall security cost-benefit analysis according to specific security countermeasures
- Makes use of a familiar tool
- Provides statistical modeling to allow for the variable nature and impact of real life security threats

Utilizing the model embraces the advantages contained within the simplicity of the ALE model, but also adds the ability to account for uncertainty through advanced statistical analysis. Effectively, this allows the decision-maker to not only view the potential return on investment of a security technology, but also to analyze the probability of achieving that return, all within the same model.

D. ADDITIONAL VALUATION OF SIEM SOLUTIONS

1. Soft Benefits

Application of a SIEM solution provides significant value to an organization that financial models fail to grasp. These soft benefits take the form of increased productivity, heightened situational awareness, broader security visibility and enhanced knowledge of the network environment (ArcSight, 2009). The value of these benefits far outweigh the costs associated with a SIEM implementation, and can further increase the value of an organization's information systems beyond what can be measured in dollars and cents.

The most valuable soft benefit of a SIEM solution, which effectively defines the entire motivation for implementing a SIEM solution, is the knowledge that a SIEM system provides about the host network. An average organization employing between 1,000 and 5,000 employees will experience an average of 81,893,882 security events per year (IBM, 2013). A security event can take the form of anything from an active network scan to an e-mail phishing attempt. However, determining the true nature of a network attack through all of those individual events is not only impractical, but also impossible. On average, a similar organization employing a SIEM solution gains the ability to sift through all of those events and discern the real network attacks from the network noise, distilling the huge amount of events down into an average of 73,400 attacks per year (IBM, 2013). Effectively, a SIEM solution exposes an enterprise to all the risk that already existed on their network that they could not previously detect (IT Business Edge, 2013). Without a SIEM solution to gather, correlate and display all of the actionable security events across a network, the majority of the attacks would have gone unnoticed.

Determining the economic value of a SIEM implementation by determining the return an investment in the technology can provide makes the endeavor economically justifiable, but it misses the true value of the solution. SIEM systems may never deliver a return on investment in the strictest of sense, but they can deliver quantifiable value after the decision to invest in the technology. The value generated by a SIEM system in terms of minimized risk and cost avoidance are only magnified by the value provided to an enterprise from increased knowledge of their information systems in addition to process and workflow efficiencies (RSA – ROI).

2. Compliance

SIEM solutions also provide additional value to an enterprise through their ability to assist in maintaining and enforcing compliance requirements in accordance with established regulations and legislation. Most notably, SIEM

implementations are able to account for the majority of requirements placed on organizations with respect to log management, reporting requirements, as well as requirements for advanced security. Furthermore, SIEM systems also increase the capability of IT staff with respect to log management and archival, reducing the amount of time, cost and effort required to meet the requirements mandated by regulation (RSA – ROI).

3. Productivity

SIEM solutions also add value to the enterprise by increasing the productivity of both employees and network assets. SIEM systems allow organizations to automate a large portion of their information system management responsibilities, reducing the costs of device management (Prism Microsystems, 2007). This reduction in demand on staff to accomplish device management tasks could even reduce costs further by allowing organizations to do more with less people. However, if an organization is already doing more with less, the increased productivity of staff allows them to accomplish more without increasing the headcount (RSA – ROI). Additionally, SIEM solutions also assist in reducing the number of support calls to internal help desks as well as reduce the rime required to solve issues by providing better diagnostic tools, thereby preventing or predicting disruption (Prism Microsystems, 2007).

Maintaining availability to network assets by preventing resource outages also increases the productivity of an organization by reducing staff downtime. The automated event management provided by SIEM solutions allows organizations to avoid disruptions from security incidents or network events while at the same time provides the ability to “resolve issues more quickly, thereby reducing overall impact on the user community and improving business continuity” (Prism Microsystems, 2007). Additionally, because SIEM systems provide immediate notification of critical events and trends, organizations can shift to a proactive stance instead of a reactive stance, avoiding system failure and improving network functionality.

E. CASE STUDIES

1. Background

The following cases describe success stories of organizations that implemented a SIEM solution within their network environment. They detail both the intended application of the system, the return on investment achieved after the investment in a SIEM application, and also many cases of added value that the system provided.

2. Security Event Management

A mid-size organization implemented a SIEM system to initially monitor 40% of their network. After four months the system detected more security events than all other detection methods combined (Thurman, 2011). Proactively detecting these threats also saved on help desk costs and lost productivity.

An organization implementing HP ArcSight's SIEM system saw a reduction of their critical incident rate to fewer than 200 per hour, representing a decrease of over 93% (ArcSight, 2009). Additionally, the improved detective capability allowed the organization to repurpose 75% of their IT security staff to strategic efforts (ArcSight, 2009).

Using new intelligence gathered from a SIEM system a "firm's anti-fraud team was able to stop illegitimate bank transfers worth nearly $900,000 within the first week. The combination of real-time correlation and pin-point accuracy allowed the bank to find and stop these transactions, translating to a payback period of less than a week" (ArcSight, 2009).

A national cooking supply company has been able to cut half the time it takes to perform a security audit, and reduced their incident response time by 75% (RSA – ROI).

3. Increased Productivity

"A financial institution realized significant manpower savings on incident handling and forensic analysis. In one example, a denial of access investigation that used to take the company's security analysts four days took ten minutes" (RSA – ROI).

"A large U.S. financial institution with strict log retention requirements was able to save 80% of their file share disk space and the man hours associated with log purging and maintenance issues" (RSA – ROI).

An organization was able to reduce personnel expansion by approximately 85% over three years based on increased productivity of existing staff, effectively recovering the SIEM investment in a little more than three months due to the cost savings on staff (ArcSight, 2009).

4. Regulatory Compliance

A U.S. based retailer realized a 60% savings in the time it spent meeting SOX and PCI requirements (RSA, 2009).

A regional utility company estimated that it spent over 8,500 man-hours at a cost of approximately $1.5 million dollars preparing for their SOX audit. After implementation of a SIEM solution, their total time required to prepare for the audit was reduced to only 900 hours—"a reduction of nearly 90%. The cost savings on the effort resulted in a payback period of the SIEM investment of just 39 days (ArcSight, 2009).

In order to meet UK Government security auditing standards, a UK-based service provider estimated that it required six man-years each year to manually extract and review the required logs. After the implementation of a SIEM solution, the system made it possible for a single staff member to meet all required obligations while only spending four hours per week on the assignment (RSA, 2009).

5. Other Sources of Value

While monitoring call center representative behavior, ArcSight discovered an unusually heavy use of printing resources – roughly a million pages at a cost of about $100,000 in printer lease, paper and toner cartridges each month. A quick investigation unveiled the fact that most of the employees were also students and were using the organization's resources to print textbooks, papers and a host of material unrelated to their job. This analysis alone demonstrated an ArcSight ESM investment payback period of just 2 ½ months, and the on-going savings have paid back the initial SIEM outlay many times over. (ArcSight, 2009)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. APPLICATION OF INFORMATION SECURITY ROI MODELS TO A SIEM SOLUTION IN A NOTIONAL DOD ENVIRONMENT

A. ASSUMPTIONS

1. Single-Point Estimate Models

Calculating the potential return on investment for SIEM solutions requires the use of several basic assumptions in order to effectively apply a single-point estimation model examining potential cost savings. Utilizing this model will adhere to the following assumptions:

- The number of security incidents will follow the trend set forth in the report GAO-12–666T filed by the United States Government Accountability Office describing current cyber security threats facing the nation. This trend shows a growth rate in the number of cyber security incidents across federal agencies of approximately 680% every five years. According to this trend, Table 1 shows the projected number of cyber security incidents reported by federal agencies for the next five years based on existing data. (Wilshusen, 2012)

Year	Number of Federal Agencies	Number of DoD Agencies	Percentage of DoD Agencies	Number of Incidents	Number of Incidents in DoD Agencies	Incident Per DoD Agency
2006	1,300	82	6.31%	5,503	347.11	4.23
2007	1,300	82	6.31%	12,980	818.74	9.98
2008	1,300	82	6.31%	20,457	1,290.36	15.74
2009	1,300	82	6.31%	27,933	1,761.93	21.49
2010	1,300	82	6.31%	35,410	2,233.55	27.24
2011	1,300	82	6.31%	42,887	2,705.18	32.99
2012	1,300	82	6.31%	101,213	6,384.20	77.86
2013	1,300	82	6.31%	159,539	10,063.23	122.72
2014	1,300	82	6.31%	217,866	13,742.32	167.59
2015	1,300	82	6.31%	276,192	17,421.34	212.46
2016	1,300	82	6.31%	334,518	21,100.37	257.32
2017	1,300	82	6.31%	454,944.48	28,696.50	349.96

Table 1. Number of Cyber Incidents Against Federal Agencies Reported to U.S. CERT

- The Ponemon Institutes 2012 report on the cost of cyber crime estimated that the annual cost of successful cyber attacks in the United States is approximately $8.9 million. Furthermore, this institute determined a weekly successful attack rate of 102 attacks

per week. Utilizing this annual rate, one can assume that an annual average of 5,304 successful attacks. From this, it can be assumed that the average cost of a single incident is approximately $1,684.30. Table 2 demonstrates this understanding. (Ponemon, 2012)

Average Annual Cost of Cyber Crime	$8,933,510.00
Weekly Attack Rate	102
Annual Attack Rate	5,304
Average Cost of Single Incident	$1,684.30

Table 2. Average Cost of a Single Cyber Incident

- The Ponemon Institute estimates that the average time required to resolve a successful cyber attack is 18 days (Ponemon, 2012). This constitutes approximately 192 working hours.
- The employment of a mid-size DoD enterprise is estimated at consisting of approximately 1,000 people. Assuming a ratio of commissioned officers to enlisted personnel of 5:1, and applying a hierarchical pay scale based on published pay rates for military personnel available from the Defense Finance and Accounting Service (DFAS), the average hourly income of a single staff member equates to approximately $40 per hour.
- In order to simplify the compliance reporting requirements on each DoD agency, the model utilizes a minimum of twelve annual reports, as defined by White House Memorandum M-12–20 outlining the FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (ZIENTS, 2012).

B. COST REDUCTION

1. Model Description

The basic single-point estimation model utilized in this study follows the basic components of the Alinean ROI tool (HP, 2012). The model examines cost savings as a source of return on investment, determining a conservative, probable and optimistic estimate based on the effectiveness of the security solution. This research will attempt to determine an estimate of potential ROI

utilizing this model in the areas of network vulnerability discovery, integrated threat detection, automated containment and detection, productivity and compliance reporting. This study has determined that these areas are the most valuable aspects of a SIEM solution in a DoD environment.

2. Increased Network-Based Vulnerability Discovery

One of the primary benefits of a SIEM solution is the advanced security capability drawn from the intelligence gathered from disparate network security devices. As a result, the overall effectiveness of the network security architecture increases. This is particularly the case when initially deploying a SIEM solution and discovering all of the risk that a network is exposed to but was previously unknown. Table 3 shows the estimated cost savings of a SIEM solution based on its ability to affect change in the annual number of successful network based attacks. Assuming an average cost incurred on the organization of a successful network attack equals approximately $1,684.30, and that the number of successful network based attacks reported by DoD agencies in 2012 is approximately 122, the total cost of these attacks equals over $200,000.

Estimating this cost after implementation of a SIEM solution shows an incredible amount of cost savings, compared to the untreated cost of $206,697.30. Even a conservative estimate shows a potential reduction in successful attacks of 20% resulting in a cost savings of over $40,000. Additionally, following the assumed increase in successful attacks shows even greater reduction in costs over the next five years. Ultimately, the even the conservative estimates point to an immediate costs savings of approximately $41,339.46 to $186,027.57 in the first year, depending on the effectiveness of the deployed solution.

Increased Network-Based Vulnerability Discovery						
Increased Network-Based Vulnerability Discovery		Current (As Is) Value	Transform (As Is to To Be)	Conservative	Probable	Optimistic
A	Average Cost of Successful Network Based Vulnerability	$1,684.30	Absolute Value	$1,684.30	$1,684.30	$1,684.30
B	Number of Annual Network Based Attacks	122.72	Percentage Change	-20.00%	-50.00%	-90.00%
				98.176	61.36	12.272
Total Annual (A * B)		$206,697.30		$165,357.84	$103,348.65	$20,669.73

Ideal Benefits [Current (As Is) - Transformed (To Be)]	Year 1	Year 2	Year 3	Year 4	Year 5
Conservative	$41,339.46	$56,454.37	$71,569.28	$86,680.82	$117,887.53
Probable	$103,348.65	$141,135.92	$178,923.19	$216,702.04	$294,718.81
Optimistic	$186,027.57	$254,044.65	$322,061.74	$390,063.67	$530,493.87

Average Annual Benefit Increase (Starting Year 2)	127.96%

Table 3. Potential Cost Savings of Increased Network-Based Vulnerability Discovery

3. Integrated Threat Detector

In addition to discovering threats that were previously unknown, SIEM solutions effectively increase the capability of existing network security devices by correlating events across them, distilling threat patterns and detecting low volume intrusion attempts. In order to reflect this increase in capability, the point-estimate model assumes a percentage change in the number of successful network attacks ranging from a conservative estimate of a 10% decrease, to an optimistic estimate of a 30% decrease.

Utilizing these projected decreases in successful attacks as well as data drawn from CERT statistics and the Ponemon Institute to determine the average number of successful attack and the average cost of attack, Table 4 shows the potential cost savings of a SIEM solution. These estimates are based on the reduction of successful attacks due to the ability of SIEM solutions to actively detect attacks in real or near real-time through aggregation and correlation of log data from various network security devices. The conservative estimate shows potential savings ranging from $20,669.73 to $62,009.19 in the first year of deployment. Furthermore, based on successful attack projections for the next five years, the cost savings benefit is projected to increase at a rate of approximately 128%.

Integrated Threat Detector						
Integrated Threat Detector		Current (As Is) Value	Transform (As Is to To Be)	Conservative	Probable	Optimistic
A	Number of Annual Network Based Attacks	122.72	Percentage Change	-10.00%	-20.00%	-30.00%
				110.45	98.18	85.90
B	Average Cost of Successful Network Based Vulnerability	$1,684.30	Absolute Value	$1,684.30	$1,684.30	$1,684.30
Total Annual (A * B)		$206,697.30		$186,027.57	$165,357.84	$144,688.11

Ideal Benefits [Current (As Is) - Transformed (To Be)]	Year 1	Year 2	Year 3	Year 4	Year 5
Conservative	$20,669.73	$28,227.18	$35,784.64	$43,340.41	$58,943.76
Probable	$41,339.46	$56,454.37	$71,569.28	$86,680.82	$117,887.53
Optimistic	$62,009.19	$84,681.55	$107,353.91	$130,021.22	$176,831.29

Average Annual Benefit Increase (Starting Year 2)	127.96%

Table 4. Potential Cost Savings Leveraging SIEM Integrated Threat Detection

4. Automated Detection and Containment

Another impressive security feature of SIEM applications is their ability to automatically apply mitigation efforts when a potential threat is detected. These efforts can be applied to a specific attack pattern or signature and can also increase in severity given the nature of the detected threat. For example, after detecting unauthorized access to confidential data from an internal user, the SIEM application can be configured to automatically suspend that users access to various network services. Additionally, SIEM systems also provide notification of these events in a manner consistent with their perceived threat. For example, detecting a network scan would result in a routine notification to a security analyst's inbox, whereas an active intrusion could trigger alarms and immediate notification of security staff through a variety of means.

The primary areas of concern when determining cost savings due to detection and containment protocols concern the number of successful attacks and the time taken to resolve an attack. As a result, in this model the cost savings are realized by reducing the number of successful attacks through enhanced detection methods and also reducing the average time that it takes to fully resolve an attack due to the speed of automatic procedures.

The results shown in Table 5 represent the cost savings provided by reducing the number of security incidents that security analysts respond to as well as the average time that it takes to resolve the incident. The Ponemon institute estimates that the average time taken to resolve a security incident is approximately eighteen days, which works out to about 192 working hours. Applying a fully burdened labor rate of $65 per hour to a security analyst, the potential cost savings of an SIEM solution become readily apparent. As a result of the reduction in resolution time, thanks to automated security protocols and SIEM's notification system, provides substantial cost savings by requiring less labor from security staff. Based on the conservative estimate of approximately one hundred successful attacks and a reduction of less than twenty hours to

resolve each attack, a firm can expect nearly a $500,000 cost savings. Additionally, the ability of SIEM systems to distill relevant security information from torrents of data has been proven to effectively reduce the workload of security staff significantly. Therefore, it is not unlikely that an organization could expect to see the optimistic results of this cost savings model, which could result in almost $1.5 million in savings during the first year of deployment.

Automated Detection and Containment						
Automated Detection and Containment		**Current (As Is) Value**	**Transform (As Is to To Be)**	**Conservative**	**Probable**	**Optimistic**
A	**Annual Number of Successful Exploits**	122.72	Percentage Change	-20.00%	-50.00%	-90.00%
				98.18	61.36	12.27
B	**Average Burdened labor rate for Security Analyst**	$65.00	Absolute Value	$65.00	$65.00	$65.00
C	**Average hours required by analysts to coordinate response and resolve a successful breach.**	192	Percentage Change	-10.00%	-20.00%	-30.00%
				172.8	153.6	134.4
Total Annual (A * (B * C))		$1,531,545.60		$1,102,712.83	$612,618.24	$107,208.19

Ideal Benefits [Current (As Is) - Transformed (To Be)]	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Conservative	$428,832.77	$585,626.50	$742,874.50	$899,179.01	$1,222,900.22
Probable	$918,927.36	$1,254,913.92	$1,591,873.92	$1,926,812.16	$2,620,500.48
Optimistic	$1,424,337.41	$1,945,116.58	$2,467,404.58	$3,102,635.90	$4,061,775.74

Average Annual Benefit Increase (Starting Year 2)	127.92%

Table 5. Potential Cost Savings of Automated Detection and Containment

5. End User Productivity

User productivity is measured by reducing the amount of network outage time. SIEM solutions assist in maintaining availability of network services by increasing the security capabilities of the network and also by providing network information that can be used to predict and diagnose potential issues. In this single-point estimate model, the cost savings is realized from the reduction of annual outage time, measured in hours. From this, the average hourly salary of the staff multiplied by the total number of hours that services are not available determines the cost of a network outage.

The data contained Table 6 estimates the annual outage time in hours of a DoD agency employing approximately 1,000 individuals. Current military employment ratios suggest an officer to enlisted employment ratio of approximately 1:5. As a result, the pay scheme of this organization results in an average hourly wage of approximately $45.00. Additionally, the model assumes that despite a disruption in network services, employees are able to maintain at least 50% productivity by either accomplishing other tasks or completing work offline.

The results of the model show that even a conservative reduction in downtime has the potential to save significant amounts of money across the organization. From reducing the network downtime by only twenty-five hours, from one hundred to merely seventy-five per year, the organization has the potential to realize $750,000 annually in cost savings. More likely, the loss of productivity as a result of network downtime will not result in such a sweeping reduction in productivity across every employee of an organization. However, even reducing the amount that the lack of network resource availability affects employee productivity results in significant cost savings. For example, reducing the amount of network downtime, even if the resulting average productivity reduction is only approximately 10%, the organization will still realize an annual cost savings of $150,000. As a result, the cost savings potential derived from

reduced network downtime represents the simplest and most effective means of determining the potential return on investment of a SIEM solution.

End User Productivity						
End User Productivity		**Current (As Is) Value**	**Transform (As Is to To Be)**	**Conservative**	**Probable**	**Optimistic**
A	**Number of staff affected by outage**	1000	Absolute Value	1000	1000	1000
B	**Annual outage time in hours.**	100	Percentage Change	-25.00%	-50.00%	-75.00%
				75	50	25
C	**Average Business Staff Rate/Hour**	$45.00	Absolute Value	$40.00	$40.00	$40.00
D	**Productivity Reduction due to outage.**	10%	Absolute Value	10%	10%	10%
Total Annual (A * B * C * D)		$450,000.00		$300,000.00	$200,000.00	$100,000.00

Ideal Benefits [Current (As Is) - Transformed (To Be)]	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Conservative	$150,000.00	$156,000.00	$162,240.00	$168,729.60	$175,478.78
Probable	$250,000.00	$260,000.00	$270,400.00	$281,216.00	$292,464.64
Optimistic	$350,000.00	$364,000.00	$378,560.00	$393,702.40	$409,450.50

Average Annual Benefit Increase (Starting Year 2)	4.00%

Table 6. Projected Cost Savings Based on Increased User Productivity

6. Automatic Compliance Reporting

Many regulations related to information systems and network security systems require large amounts of effort to ensure compliance with their established standards. Often, in order to achieve full compliance, organizations must submit detailed reports containing network statistics, extensive details of information system configurations or even large amounts of log data. SIEM solutions assist in maintaining full compliance with all mandated regulations by providing a simple means of compiling the required reports. The cost savings result from the decreased amount of time required to produce each of these reports.

For example, federal agencies are required to submit monthly compliance reports to U.S.-CERT through the CyberScope program (Zients, 2012). Table 7 estimates the costs associated with these efforts, assuming each report requires approximately one hundred hours of effort from a security analyst in order to gather all of the relevant log data on potential cyber attacks as well as the configurations of all of the affected systems. The estimated annual cost to produce these reports equals $78,000. Reducing the amount of time required by each analyst in the production of each report has the potential to reveal modest annual cost savings, depending on the effectiveness of the SIEM application. Effectively, the cost savings resulting from each potential reduction in work time producing compliance reports has the ability to realize anywhere from $7,800 to $23,400 annually. While this is much more modest of a cost savings than previously examined applications of a SIEM solution, it still represents additional value that a SIEM application provides to the organization.

Automatic Compliance Reporting						
Automatic Compliance Reporting		Current (As Is) Value	Transform (As Is to To Be)	Conservative	Probable	Optimistic
A	Annual number of compliance reports created	12	Absolute Value	12	12	12
B	Analyst hours spent per report	100	Percentage Change	-10%	-20%	-30%
				90	80	70
C	Average burdened labor rate for Security Analyst	$65.00	Absolute Value	$65.00	$65.00	$65.00
Total Annual (A * B * C)		$78,000.00		$70,200.00	$62,400.00	$54,600.00

Ideal Benefits [Current (As Is) - Transformed (To Be)]	Year 1	Year 2	Year 3	Year 4	Year 5
Conservative	$7,800.00	$8,112.00	$8,436.48	$8,773.94	$9,124.90
Probable	$15,600.00	$16,224.00	$16,872.96	$17,547.88	$18,249.79
Optimistic	$23,400.00	$24,336.00	$25,309.44	$26,321.82	$27,374.69

Annual Benefit Increase (Starting Year 2)	4.00%

Table 7. Potential Cost Savings Enabled through Automatic Compliance Reporting

C. RISK MANAGEMENT AND LOSS AVOIDANCE

1. Background

Many variations of the return on security investment model exist, each of which attempts to justify investment in a particular security technology based on the ability to reduce risk and avoid losses. These models all determine the return on a security investment to be equivalent to the difference between the treated and untreated losses. However, many of them fail to account for the inherent uncertainty of information security events. Effectively, the majority of the existing models base the rate of occurrence of security events on single-point averages. However, these models fail to consider the strategy or incentive of the hacker, and therefore generalize the rate of occurrence of malicious attacks. This is of particular concern to DoD agencies as DoD information systems represent a choice target.

Dr. Johnathan Mun's IT Intrusion Management model represents a risk management model that incorporates uncertainty in the rate of occurrence of attacks. Furthermore, with the incorporation of Monte Carlo risk simulations a number of variables in the model including percentage of network affected and percentage of workforce affected, the model adds additional variation into the computation of potential losses due to cyber attacks (Mun, 2010). The model compares a current state, based on the existing security investments, against a future state based on the inclusion of new technology (Mun, 2010). The primary measurement drawn from the model is the cost associated with loss of operational productivity defined as the loss of employee working hours due to network outage.

Simplifying the model to represent a notional DoD network took several steps. Primarily, the reduction of the staff to 1,000 personnel reflects a mid-sized DoD agency in addition to providing some comparison against the single-point estimate model previously utilized. Additionally, the number of networks within the organization was reduced to two, the Non-Classified Internet Protocol Router

Network (NIPR) and Secret Internet Protocol Router (SIPR) networks, in order to simplify the model.

2. Current State Versus Future State

Examining the potential application of a SIEM solution against a current state reveals the potential cost savings the application provides in terms of productivity. According to the IT Intrusion Management model, the different classes of attacks, detailed in Appendix E, each class of attacks has a general amount of disruption that it causes on a network. Figure 2 defines the percentages that each class of attack disrupts the network and the workforce. These estimates are derived from interviews with multiple technical experts in the field of information security (Mun, 2010).

Attack Class	Network Disruption	Employee Disruption
I	10%	10%
II	20%	20%
III	35%	35%
IV	50%	50%
V	100%	100%

Figure 1. Approximate Impact of Cyber Attacks

The model also accounts for variations in these amounts as well. The future state of the model, after the implementation of a SIEM solution reduces the uncertainty of these values, as a result of the increased effectiveness of the security architecture with the addition of the SIEM application's detective and preventative capabilities. Additionally, the future state differs from the current state model in the respect that it assumes a 75% reduction in productivity loss as a result of the increased diagnostic and preventative capability inherent in the SIEM solution. Table 8 shows the comparison of impact that each attack class has on the network and the potential percentage of losses avoided by implementing the future state.

	Class I Attack	Class II Attack	Class III Attack	Class IV Attack	Class V Attack
Total Impact (CS)	23,982	101,224	320,312	865,176	3,543,059
Total Impact (FS)	7,196	35,506	119,453	316,294	1,109,765
Variance (%)	30.00%	35.08%	37.29%	36.56%	31.32%

Table 8. Estimated Cost of Cyber Attack on Current State versus Future State Security Architectures

Additionally, the IT Intrusion Management model provides a means to estimate the rate of occurrence of potential classes of attacks in order to determine the potential amount of damage incurred by a combination of attacks over a span of five years. Utilizing the most likely scenario in the model, Scenario VI, represents a more likely attack scenario experienced by DoD agencies. However, because of the inherent value of DoD information systems, they represent a much more desirable target to more advanced threats. Therefore, the rate of occurrence of each of the attack classes must be adjusted slightly to account for this. Table 9 reflects the adjusted rates of occurrence for each class of attack.

These estimations of the ARO of the classes of cyber attacks against DoD networks are inflated with respect to the ARO's associated with cyber attacks against other agencies. These inflations are based on direct observations reported from DoD agencies in addition to historical evidence of significant cyber security events. For example, the Center for Strategic and International Studies (CSIS) maintains a running list of all significant cyber security events worldwide since 2006 (CSIS, 2006). These significant events represent at least a Class IV attack or higher, as they primarily detail security events involving a determined malicious hacker or group of hackers and sometimes carry accusations of state run cyber crime. Examining the results of their research reveals that over the last seven years, eleven of the one hundred and twenty four significant cyber security events worldwide targeted either the DoD directly, or an affiliated agency. Effectively, nearly 10% of all significant cyber security events worldwide are directed at DoD agencies or their affiliated agencies. These attacks range from data breaches of personnel files or technological information on weapons

systems to the real-time interception of surveillance drone communications (Rosenzweig, 2012). Furthermore, this data supports announcements made by the Pentagon in 2012, asserting that their information systems endure approximately 10 million cyber attacks a day (Fryer-Biggs, 2012).

Attack Class	Annual Rate of Occurrence
I	80%
II	50%
III	20%
IV	5%
V	0.00441%

Table 9. Estimated Annual Rate of Occurrence of Cyber Attacks

Running the model with these adjusted rates of occurrence, the total amount of losses incurred between the current state and the future state is easily discernable. Table 10 summarizes the findings.

Effectively, over a span of five years, the impact of multiple attacks of various classes against the network is nearly one million dollars lower in the future state than the current state. At each year within the table the model calculates the total impact on both the current state and future state along with the variance and the risk adjustment between the two states. The variance refers to the percentage amount of losses avoided as a result of the implementation of the future state security architecture (Mun, 2010). The risk adjustment measures the difference between the impact on the current state and future state (Mun, 2010).

The risk adjustment value essentially captures the total potential losses that the two states are likely to endure. Additionally, comparing the risk adjustment and variance between years one through five, one can observe that even in the event of multiple successful attacks in a single year, the impact on the future state remains between 60% and 70% of the impact on the current state. Concurrently, the variance only decreases by a minimal amount as the

sophistication of the attacks increases. For example, despite only a 6.4% decrease in variance between year four and year five, the value of the risk adjustment of year four is nearly $600,000 greater, despite enduring multiple attacks of much greater magnitude.

	Most Likely Attack Scenario					
	Year 1	Year 2	Year 3	Year 4	Year 5	TOTALS
Class I Attacks	1	1	1	0	1	4
Class II Attacks	0	1	0	1	0	2
Class III Attacks	0	0	1	0	0	1
Class IV Attacks	0	0	0	1	0	1
Class V Attacks	0	0	0	0	0	0
Class I Attack Impact CS	$23,982	$23,982	$23,982	$0	$23,982	$95,929
Class I Attack Impact FS	$7,196	$7,196	$7,196	$0	$7,196	$28,782
Class II Attack Impact CS	$0	$101,224	$0	$101,224	$0	$202,447
Class II Attack Impact FD	$0	$35,506	$0	$35,506	$0	$71,012
Class III Attack Impact CS	$0	$0	$320,312	$0	$0	$320,312
Class III Attack Impact FS	$0	$0	$119,453	$0	$0	$119,453
Class IV Attack Impact CS	$0	$0	$0	$865,176	$0	$865,176
Class IV Attack Impact FS	$0	$0	$0	$316,294	$0	$316,294
Class V Attack Impact CS	$0	$0	$0	$0	$0	$0
Class V Attack Impact FS	$0	$0	$0	$0	$0	$0
Impact based on Current State	$23,982	$125,206	$344,294	$966,400	$23,982	$1,483,865
Impact based on Future State	$7,196	$42,701	$126,649	$351,800	$7,196	$535,541
Variance	70.00%	65.89%	63.22%	63.60%	70.00%	63.91%
Risk Adjustment	$16,787	$82,504	$217,646	$614,600	$16,787	$948,324

Table 10. Losses Incurred As a Result of the Most Likely Attack Scenario

Examining the distribution of total impact on the current state and future state over one thousand trials also supports the future state. Figure 2 and Figure 3 show the results from the Monte Carlo risk simulations. Estimating the most frequent impact value from both distributions shows a drastically lower value for the future state. Even the most unlikely values displayed at the far right tails of the distributions show significantly higher impacts in the current state than the

future state. Additionally, the difference between the minimum values on the far left of the distribution scales show approximately a $300,000 difference in the least likely, least costly outcomes between the current state and the future state.

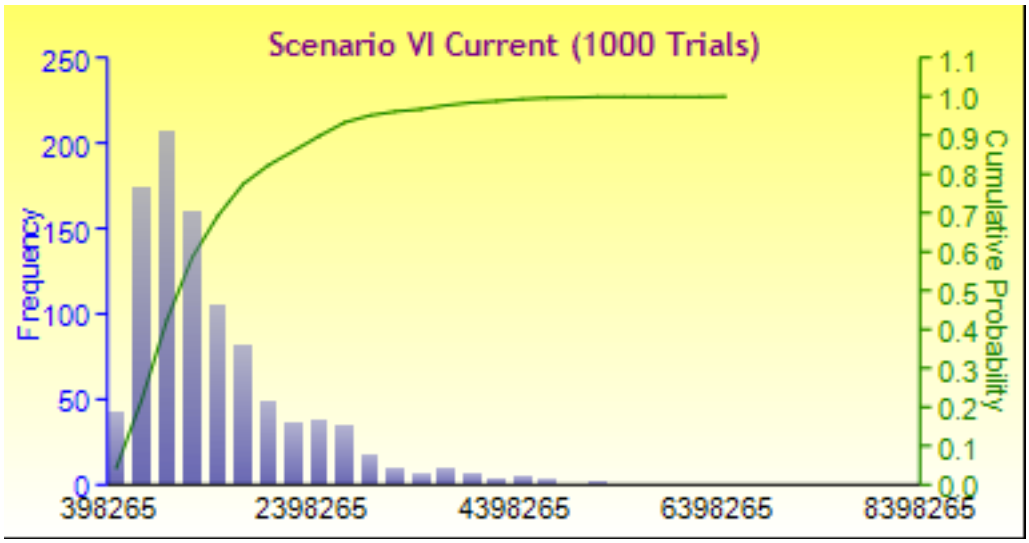

Figure 2. Distribution of Potential Impact on the Current State

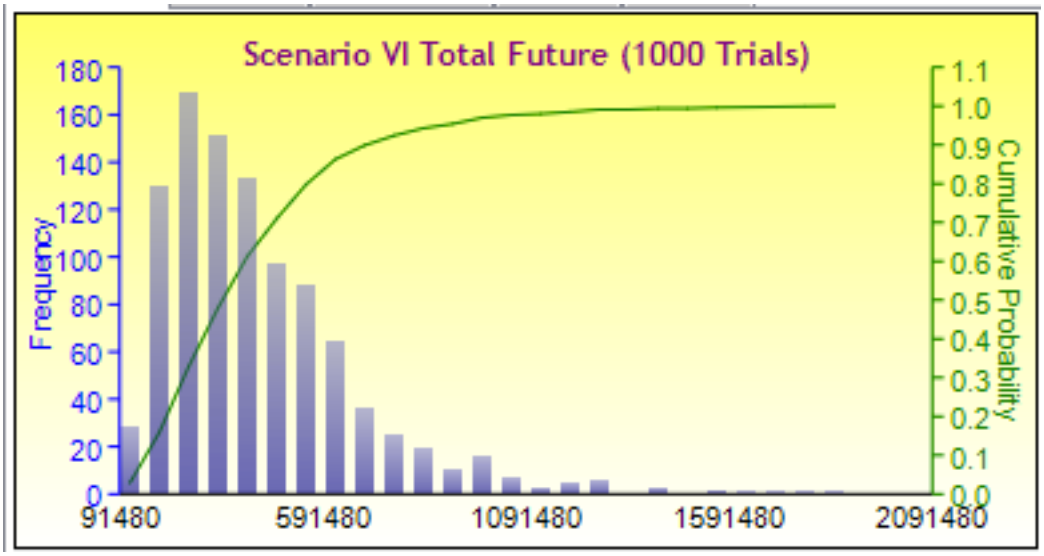

Figure 3. Distribution of the Potential Impact on the Future State

Ultimately, the distributions shown in Figure 2 and 3 shows that the future state, over one thousand simulations, is far more likely to provide significantly reduced losses. Effectively, the future state characterized by the implementation

of a SIEM solution provides much more capability in reducing risk, which in this model is primarily defined by the reduction of productivity loss on the organization. However, applying confidence intervals to the distributions in Figure 2 and Figure 3 show additional insight into the observed impacts on the future state and the current state.

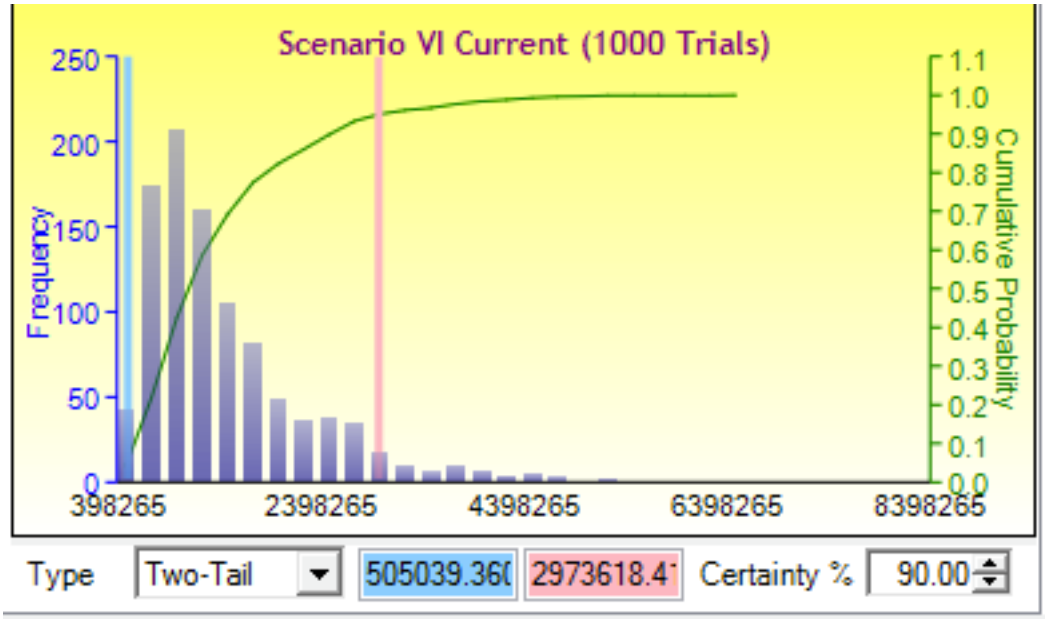

Figure 4. Distribution of Potential Impact on Current State with 90% Confidence Intervals

Figure 4 and Figure 5 show the distributions of potential impacts on the current state and future state over one thousand simulations with 90% confidence intervals. These intervals indicate, with 90% certainty, that the lowest impact on both the current state and future state will be approximately $505,039 and $125,093, respectively. Effectively, given the uncertainty of cyber attacks and their AROs, a DoD agency can expect to still endure at least $505,039 in losses in the event of the best-case scenario occurring. Conversely, the future state displays the potential to avoid nearly $400,000 in losses.

Examining the upper confidence interval reveals similar conclusions. With 90% certainty, the greatest impact on both the current state and future state is

$2,973,618 and $884,928, respectively. The difference between the significance of the upper and lower confidence intervals effectively boils down to the likelihood of enduring cyber attacks of greater magnitudes. Despite the frequency of occurrence of the observed impacts at the higher confidence level, these represent the impacts of higher classes of cyber attacks, which are of particular concern to the DoD. Effectively, the impact values at the upper 90% confidence interval represent a value close to the worst-case scenarios for both the current state and the future state. Still, the results are drastically different, showing a difference in impact of nearly two million dollars.

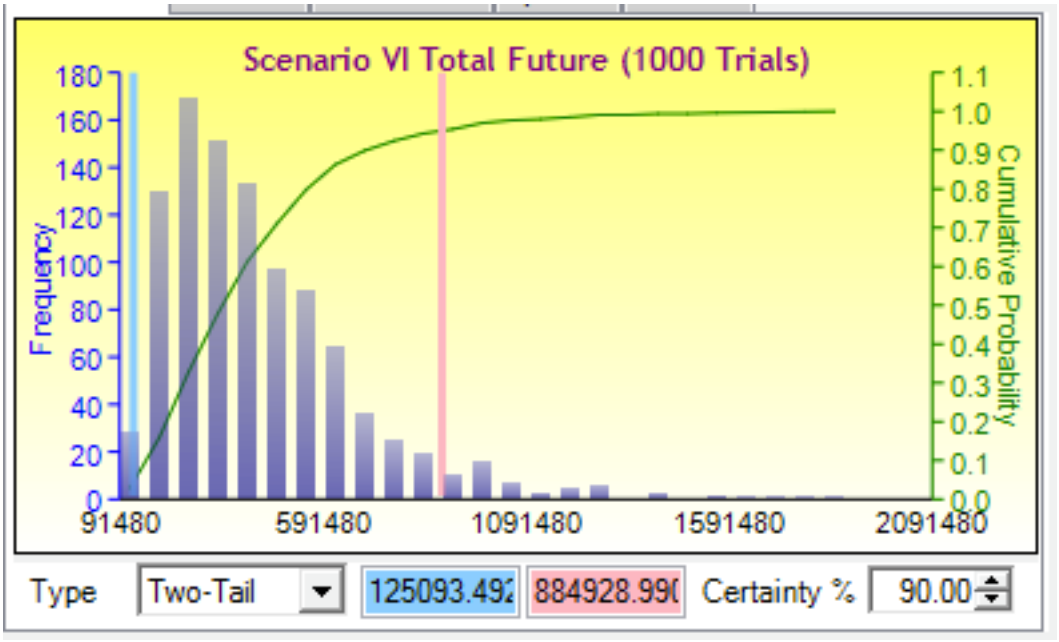

Figure 5. Distribution of Potential Impact on Future State with 90% Confidence Intervals

Applying a left-tail 95% confidence interval to the distribution reveals the greatest impact, with 95% certainty, that each state has the potential to endure. After one thousand trials, the values of these potential maximum impacts for the current state and future state are $2,973,618 and $884,928, respectively. Essentially, these values equate to the most likely worst-case scenario that either state is likely to endure.

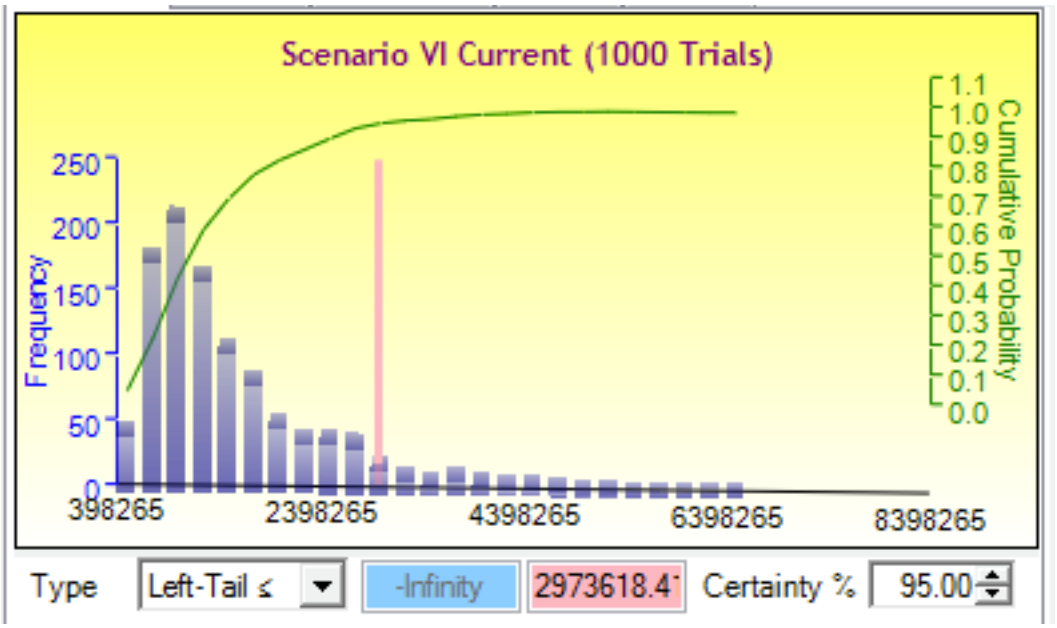

Figure 6. Distribution of Potential Impact on Current State with a Left-Tail 95% Confidence Interval

The difference between these worst-case scenarios is approximately $2,100,000. While this represents a significant difference between the potential losses avoided between the current state and future state, it does adequately reflect the amount that should be invested in the SIEM solution represented in the future state. Effectively, the 95% confidence interval suggests that the DoD could spend any amount between almost $900,000 and $2,000,000 to achieve the reduction of impact associated with the future state. However, given the sensitivity of information and data contained on DoD information networks, it is likely that the agency intends to minimize as much risk as possible.

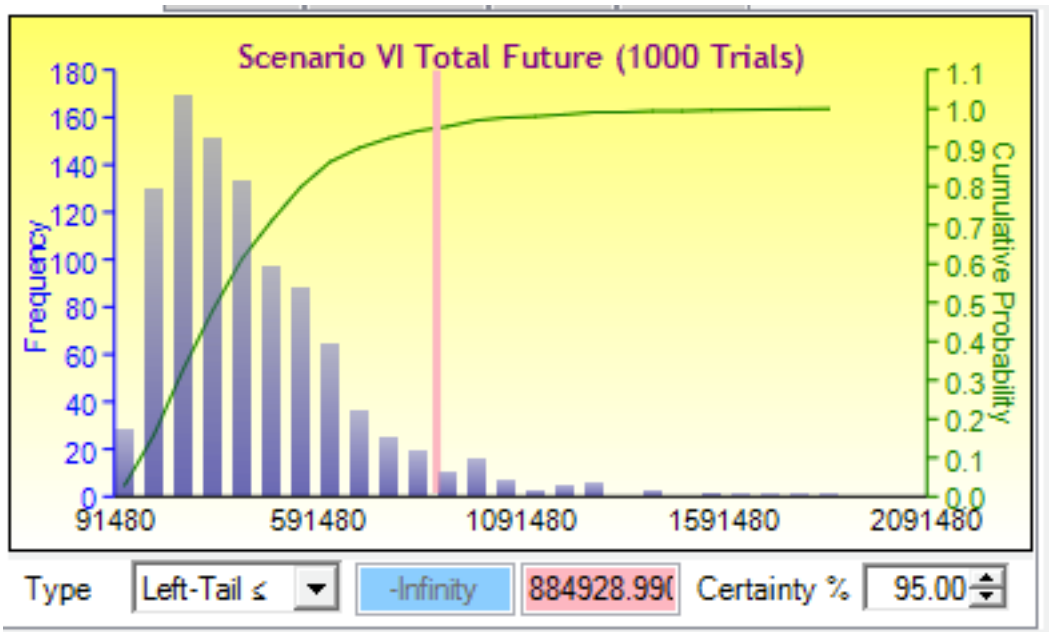

Figure 7. Distribution of Potential Impact on Future State with a Left-Tail 95% Confidence Interval

V. CONCLUSIONS

A. POTENTIAL RISKS

Application of a SIEM solution to any network environment carries its own internal risks, in addition to the pressure of economically justifying the investment. Primarily the concerns surrounding a SIEM deployment revolve around the amount of data to which the system has access. In order to effectively utilize the SIEM correlation capability, the system must aggregate data from as many sources as possible. However, in a DoD network environment, data sharing among various sources could potentially leak sensitive information. Additionally, the added bandwidth requirement to moves these large data files across the network could slow down critical network segments that support combat operations.

The potential benefits of a SIEM solution in a DoD environment, however, far outweigh the implementation risks. Effective mitigation of advanced cyber threats requires broader utilization of existing network security technologies as well as the application of systems that can correlate data across these devices. An organization like the DoD that represents a choice target for emerging sophisticated threats, including state supported threats, requires the ability to mitigate the risks of these threats quickly and effectively. The advanced security capabilities offered by SIEM solution in addition to the value that they extract from existing investments more than justifies their implementation in a DoD environment.

B. LIMITATIONS

1. Current Study

Potential limitations of this study revolve primarily around the inclusion of single-point estimates in costing models and the inability to accurately account for the targeting subjectivity of advanced cyber threats. While flawed, the use of single-point estimates in the model represents an assumption of the costs or

frequencies associated with specific security events. For example, it cannot be accurate estimated that each class I security incident will cause exactly five hours of productivity loss per employee in an organization, nor can it be stated with a large amount of certainty that a class V attack will not happen every year. This is especially true given the targeting propensity that state sponsored hackers show toward DoD agencies.

Despite the limitations of these models, they still show the potential cost savings and risk mitigation that a SIEM solution can provide. Additionally, even the most conservative estimates still show a large amount of risk and cost avoidance. However, the current study is limited by the amount of data comprising the specifics of observed cyber incidents against DoD agencies. If given enough access to historical data of cyber security incidents at DoD agencies, or even the ability to observe actual rates of occurrence of lesser classes of cyber attacks, the information presented in the models could prove more accurate in determining the potential return on investment of a SIEM solution in a DoD environment.

2. Future Study

The potential for future research in the field of advanced security intelligence on DoD networks is growing at a nearly exponential rate. With the nearly exponential increase in cyber security incidents over the last decade and the realization that agencies are under the threat of state supported cyber threats, the need for advanced detective and predictive capabilities offered by SIEM applications cannot be understated. If given the opportunity and the finances, the application of a SIEM application in a DoD environment as an experiment could have reaching affects with respect to the understanding of exactly what risks DoD information systems are exposed. Effectively, the observation of an experimental SIEM system in a DoD environment has the potential to justify the investment in the technology, if only for the network knowledge it will provide.

C. POTENTIAL BENEFITS

1. Advanced Security Intelligence

The evolution of cyber threats represents a nearly exponential growth in the amount of risk endured by most networks. Advanced threats have the ability to selectively bypass security measures and go undetected for an indeterminate amount of time, and in some cases years. Employing point security devices to counter these threats fails to consider the malicious insider, or the likelihood that an attacker can bypass these devices, and implementing a single device to counter a specific threat is not economically justifiable.

Implementation of an advanced security intelligence system, like a SIEM application, is one of the few means available to effectively thwart advanced cyber threats. The systems offer incredible security capabilities, leverage the inherent value of existing investments, and provide significant knowledge of the host network. The return that a SIEM system provides leverages all three of these aspects, providing a sophisticated security system adept at countering sophisticated threats.

2. Functional Value

The most apparent value that a SIEM solution provides to a network environment is the ability to directly observe the actual risk that the network is exposed to, rather than the perceived risks. There are too many surveys and studies in existence that reveal the assumption of adequate IT security amongst civilian organizations and DoD agencies. Without the ability to monitor the network in real time, and the ability to detect sophisticated threats before they become stubbornly lodged in sensitive information systems, placing the information security in the hands of perimeter devices or IDS/IPS systems is foolhardy. Effectively, this methodology is akin to assuming that a security guard has the ability to deter any available threat through his own perception of events, without the aid of surveillance or additional assistance. Understanding the true

risk that computer networks are exposed to is essential to deterring the advanced threats that permeate the network environment worldwide.

APPENDIX A. ATTACK CLASSES

Attack Class	Severity Level of Attack	Type of Attack	Extent of Damage	Recovery Approach
Class I	Average	Benign worm, Trojan horse, virus, or equivalent	Limited. Most damage occurs at host level.	Mostly automated, but may require some human intervention.
Class II	Slightly above average	Worm, Trojan horse, virus, or equivalent designed to create some damage or consume resources	Limited. Damage can occur at the host and network level.	Human intervention is required. Humans use tools that require interaction and expertise.
Class III	Moderately above average	Worm, Trojan horse, or equivalent designed to create significant damage and consume resources	Noticeable damage at host and network levels. Automated tools have limited effect to combat attacker.	Significant human intervention is required. Personnel require physical access to host machines and network environments.
Class IV	Significantly above average	Concentrated attack by hacker using a variety of tools and techniques to compromise systems	Significant damage to important/ sensitive data. May also include damage to host machines as Trojans and other tools are used to circumvent detection and mitigation techniques.	Extensive human intervention is required. Data and systems recovery is necessary. Multiple techniques and methods are necessary to fully recover.
Class V	Extreme case	Concentrated attack by hacker or groups of hackers who are trying to compromise infor-mation/systems and have malicious intent	Critical damage to important/sensitive information. Irreversible damage to systems/ hardware.	Extensive human intervention is required. External experts are required to assess and recover environment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. IMPACT ON CURRENT STATE

ATTACK MODELS
CURRENT STATE

	CLASS I ATTACK	CLASS II ATTACK	CLASS III ATTACK	CLASS IV ATTACK	CLASS V ATTACK
	Average	Slightly Above Average	Moderately Above Average	Significantly Above Average	Extreme Case
ENVIRONMENT DETAILS					
# Of Networks	2	2	2	2	2
Employee Headcount	1000	1000	1000	1000	1000
ESTIMATED IMPACT TO ENVIRONMENTS					
% of Network Impacted	10%	20%	35%	50%	100%
% of Employees Impacted	10%	20%	35%	50%	100%
Total Networks Down	0.20	0.40	0.70	1.00	2.00
Total Employees Impacted	100	200	350	500	1000
OPERATIONAL/PRODUCTIVITY IMPACT					
Avg. Salary/Employee (fully burdened)	$75,000	$75,000	$75,000	$75,000	$75,000
Productivity Loss (hours/employee)	5.00	8.00	12.00	24.00	72.00
Productivity Cost/hour	$36.76	$36.76	$36.76	$36.76	$36.76
Impact to Operational Productivity	$18,382	$58,824	$154,412	$441,176	$2,647,059
EMPLOYEE RECOVERY COSTS					
Costs to Recover/Employee	$50	$100	$150	$200	$200
Hours to Recover/Employee	1.00	2.00	3.00	4.00	4.00
Total Costs to Recover Employees	$5,000	$40,000	$157,500	$400,000	$800,000
NETWORK & SYSTEMS RECOVERY COSTS					
Assumption -- Hours to Recover	12	24	48	96	192
Resources per network	5	5	5	5	5
Cost per Hour	$50	$50	$50	$50	$50
Total Costs to Recover Networks	$600	$2,400	$8,400	$24,000	$96,000
TOTAL FINANCIAL LOSSES	**$23,382**	**$98,824**	**$311,912**	**$841,176**	**$3,447,059**
ADJUSTED TOTAL FINANCIAL LOSSES	$23,982	$101,224	$320,312	$865,176	$3,543,059
VARIANCE (%)	102.57%	102.43%	102.69%	102.85%	102.78%

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. IMPACT ON FUTURE STATE

ATTACK MODELS
FUTURE STATE

	CLASS I ATTACK	CLASS II ATTACK	CLASS III ATTACK	CLASS IV ATTACK	CLASS V ATTACK
	Average	Slightly Above Average	Moderately Above Average	Significantly Above Average	Extreme Case
ENVIRONMENT DETAILS					
# Of Networks	2	2	2	2	2
Employee Headcount	1000	1000	1000	1000	1000
ESTIMATED IMPACT TO ENVIRONMENTS					
% of Network Impacted	10%	20%	35%	50%	100%
% of Employees Impacted	10%	20%	35%	50%	100%
Total Networks Down	0.20	0.40	0.70	1.00	2.00
Total Employees Impacted	100	200	350	500	1000
OPERATIONAL/PRODUCTIVITY IMPACT					
Avg. Salary/Employee (fully burdened)	$75,000	$75,000	$75,000	$75,000	$75,000
Productivity Loss (hours/employee)	1.25	2.00	3.00	6.00	18.00
Productivity Cost/hour	$36.76	$36.76	$36.76	$36.76	$36.76
Impact to Operational Productivity	$4,596	$14,706	$38,603	$110,294	$661,765
EMPLOYEE RECOVERY COSTS					
Costs to Recover/Employee	$50	$100	$150	$200	$200
Hours to Recover/Employee	0.50	1.00	1.50	2.00	2.00
Total Costs to Recover Employees	$2,500	$20,000	$78,750	$200,000	$400,000
NETWORK & SYSTEMS RECOVERY COSTS					
Assumption -- Hours to Recover	2.00	8.00	12.00	24.00	96.00
Resources per network	5	5	5	5	5
Cost per Hour	$50	$50	$50	$50	$50
Costs to Recover Networks	$100	$800	$2,100	$6,000	$48,000
TOTAL FINANCIAL LOSSES	**$7,096**	**$34,706**	**$117,353**	**$310,294**	**$1,061,765**
ADJUSTED TOTAL FINANCIAL LOSSES	$7,196	$35,506	$119,453	$316,294	$1,109,765
VARIANCE (%)	101.41%	102.31%	101.79%	101.93%	104.52%

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Aguirre, I., & Alonso, S. (2012). Improving the automation of security information management: A collaborative approach. *Security & Privacy, IEEE*, (February), 55–59. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6060795

ArcSight. (2009). Demonstrating the ROI for SIEM: Tales from the trenches. Retrieved from http://h71028.www7.hp.com/enterprise/downloads/software/Demonstrating%20the%20ROI%20for%20SIEM.pdf

Butler, M. J. (2009). Benchmarking security information event management (SIEM). Retrieved from http://www.sans.org/reading_room/analysts_program/eventMgt_Feb09.pdf

Cavusoglu, H. (2003). *The economics of information technology security*. University of Texas. Retrieved from http://en.scientificcommons.org/9014179

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87–92. Retrieved from http://dl.acm.org/citation.cfm?id=1005828

Center for Strategic and International Studies. (2013). *Significant cyber incidents since 2006*. Retrieved from http://csis.org/publication/cyber-events-2006

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651–661. doi:10.1016/j.dss.2010.08.017

Chuvakin, A. (2004). Security event analysis through correlation. *Information Systems Security*, 13–18. Retrieved from http://www.tandfonline.com/doi/abs/10.1201/1086/44312.13.2.20040501/81648.3

Chuvakin, Anton. (2010). The complete guide to log and event management. Retrieved from http://www.novell.com/docrep/2010/03/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf

Constantine, L. (2011). From virtual digits to real destruction: Lessons from Stuxnet. *Cutter IT Journal*, *24*(5), 6.

Department of Homeland Security. (2003). *The National Strategy to Secure Cyberspace*. Retrieved from http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberspace_strategy[1].pdf

Dorigo, S. (2012). *Security information and event management*. Radboud University Nijmegen. Retrieved from http://www.ru.nl/publish/pages/578936/thesis_sander_dorigo.pdf

Fryer-Biggs, Z. (2012). U. S. military goes on cyber offensive. Retrieved June 12, 2013, from http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive

Honan, B. (2012). 10 steps for early incident detection. Retrieved from http://www.tripwire.com/register/10-steps-for-early-incident-detection/

Hutton, N. (2007). Preparing for security event management. *Three Sixty Information Security*. Retrieved from http://www.infosecwriters.com/text_resources/pdf/360is-prep-sem.pdf

IANS Research. (2011). The ROS of Q1 Labs' QRadar © Security Intelligence Platform. Retrieved from http://q1labs.com/resource-center/white-papers/details.aspx?id=113

IBM Security Services. (2013). IBM security services cyber security intelligence Index. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/se303058usen/SE303058USEN.PDF

Iheagwara, C. (2004). The effect of intrusion detection management methods on the return on investment. *Computers & Security*, *23*(3), 213–228. doi:10.1016/j.cose.2003.09.006

IT Business Edge. (2013). Tracking the cost, risk impact of security information and event tracking. Retrieved April 17, 2013, from http://www.itbusinessedge.com/cm/blogs/itdownloads/tracking-the-cost-risk-impact-of-security-information-and-event-tracking/?cs=48932

Karlzén, H. (2009). An analysis of security information and event management systems-The use of SIEMs for log collection, management and analysis, (January). Retrieved from http://publications.lib.chalmers.se/publication/89572

Lockstep Consulting. (2004). A guide for government agencies calculating return on security investment. Retrieved from http://www.services.nsw.gov.au/sites/default/files/ROSI Guideline SGW (2.2) Lockstep.pdf

Mun, J. (2006). *Modeling risk: Applying monte carlo simulation, real options analysis, forecasting, and optimization techniques*. Wiley.

National Institute of Standards and Technology. (2002). FISMA Overview, (December). Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

National Institute of Standards and Technology. (2013). *Special Publication 800–53: Security and privacy controls for federal information systems and organizations*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800–53r4

Office of the Secretary of Defense. (2011a). Department of Defense (DoD) information technology (IT) enterprise strategy and roadmap, (September). Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

Office of the Secretary of Defense. (2011b). *Department of Defense strategy for operating in cyberspace*. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Office of the Secretary of Defense. (2013). The budget for Fiscal Year 2013. Retrieved from http://www.google.com/url?sa=t&rct=j&q=department%20of%20defense%20budget%20for%20fiscal%20year%202013&source=web&cd=3&ved=0CDkQFjAC&url=http%3A%2F%2Fwww.aau.edu%2FWorkArea%2Flinkit.aspx%3FLinkIdentifier%3Did%26ItemID%3D13038&ei=bcLJUY23NeinigKpvYHoDw&usg=AFQjCNGeN-ikHh5yRMB71jp8oKiksKd8Iw&sig2=eZuu9-yKbGlfKTsiljwEYg&bvm=bv.48340889,d.cGE

Prism Microsystems. (2007). The business case for automated event log management. Retrieved from http://www.eventtracker.com/wp-content/uploads/2012/02/LogManagementROI.pdf

Purser, S. a. (2004). Improving the ROI of the security management process. *Computers & Security*, *23*(7), 542–546. doi:10.1016/j.cose.2004.09.004

Rosenquist, M. (2007). Measuring the return on IT security investments. Retrieved from http://communities.intel.com/servlet/JiveServlet/previewBody/1279–102–1-1305/Measuring the Return on IT Security Investments.pdf

Rosenzweig, P. (2012). Significant cyber attacks on federal systems — 2004-present. *Lawfare*. Retrieved June 12, 2013, from http://www.lawfareblog.com/2012/05/significant-cyber-attacks-on-federal-systems-2004-present/

RSA. (n.d.). Security information and event management: Expectations for mid-sized organizations. Retrieved from http://www.rsa.com/products/envision/wp/10951_ENSMB_WP_0510.pdf

RSA. (2009). ROI and SIEM. Retrieved from http://www.enterprisemanagement360.com/wp-content/files_mf/case_study/10224_ENVROI_WP_0509–1.pdf

RSA. (2011). RSA Security Management: An integrated approach to risk, operations and incident management. Retrieved from http://www.rsa.com/products/sms/sb/11420_SIMEGRC_SB_0311.pdf

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and …*, *38*(1), 55–66. Retrieved from http://sonnenreich.com/wes/return_on_security_investment.pdf

Stephenson, P. (2012). SIEM. *SC Magazine*, *23*(4), 34. Retrieved from http://search.proquest.com/docview/1011329867?accountid=12702

Swift, D. (2006). A practical application of SIM/SEM/SIEM automating threat identification. *The SANS Institute InfoSec Reading Room*.

Tarzey, B., & Longbottom, C. (2012). Advanced cyber-security intelligence, (July). Retrieved from http://www.quocirca.com/media/reports/072012/724/Quocirca - Advanced security intelligence - July 2012 - final.pdf

The Ponemon Institute. (2012). *2012 cost of cyber crime study : United States*. Retrieved from http://www.ponemon.org/library/2012-cost-of-cyber-crime-study

Thurman, M. (2011). Tracking the ROI on SIEM. *Computerworld*, 2011. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Tracking+the+ROI+on+SIEM#0

Tripwire. (2012). Supercharging incident detection. Retrieved from http://www.tripwire.com/register/supercharging-incident-detection/

Wilshusen, G. C. (2010). Continued attention is needed to protect federal information systems from evolving threats. Retrieved from http://www.gao.gov/new.items/d10834t.pdf

Wilshusen, G. C. (2012). *Threats Impacting the Nation*. Retrieved from http://www.gao.gov/products/GAO-12–666T

Zients, J. D. (2012). *FY 2012 reporting instructions for the Federal Information Security Management Act and Agency Privacy Management*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12–20.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California